Homeland Security

Daily Open Source Infrastructure Report for 18 May 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

For information, click here: http://www.dhs.gov

Top Stories

- The Louisville Courier-Journal reports that emergency crews were not able to get ammonia out of the American Cold Storage facility in Louisville, Kentucky two days after the gas leak killed two workers on May 13. (See item **3**)
- According to the New York Daily News, the New York City Police Department has crushed a sophisticated identity theft ring that wrecked the credit of 6,000 victims and bilked banks out of $15 million in bogus charges. The scam, which stretched from New York to Nigeria, is one of the largest operations of its kind dismantled by the NYPD, the police commissioner said on May 14. (See item **9**)

Fast Jump Menu

Energy Sector

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

1. *May 15, Associated Press* – (Indiana; Missouri; Oklahoma) **Flash flooding hits northern Missouri.** Several roads in north-central Missouri are closed because of flash flooding as storms move through the region. The Missouri Department of Transportation

reports road closings Friday in Mercer, Sullivan, Putnam, and Adair counties because of high water. Violent storms tore through four Midwestern states, killing three people in northern Missouri, damaging hundreds of homes, and leaving thousands without power. Authorities reported at least two tornadoes touching down in Adair County, Missouri, the first hitting Novinger just before 6 p.m. Wednesday. The Kirksville-area tornado damaged at least 60 buildings, including a car dealership on the northern edge of town where employees arrived Thursday morning to a parking lot littered with overturned vehicles and a showroom with 12-foot-high plate glass windows completely blown away. An additional 150 buildings in the county also were damaged, and that number was expected to go up. Utility provider AmerenUE reported roughly 2,600 customers without power immediately after the storms. In Oklahoma, dozens of inmates were evacuated from the Caddo County jail because of a gas line break, said the Caddo County Emergency Management director. In northeast Oklahoma, a 100 mph wind gust was recorded west of the Bartlesville airport in Washington County. The high winds downed trees and power lines, with 8,000 power outages reported at one point. Central Indiana saw wind gusts of up to 60 mph and street flooding was reported in Vincennes, Linton, and Rockville, authorities said. Utilities reported 8,000 were without power in and around Indianapolis early Thursday.
Source: http://www.kansascity.com/news/breaking_news/story/1199229.html
See also: http://www.cattlenetwork.com/top40_Content.asp?ContentID=314820

2. *May 15, Daily Sound* – (California) **Venoco applies for onshore pipeline.** For years Venoco has said it would build a pipeline on the condition that its offshore oil leases at Platform Holly were expanded, allowing the company to drill for additional oil. But with that proposal lagging in the environmental review process, and a June 1 State Lands Commission meeting, at which the barging activity is expected to come under fire, Venoco proactively sprung for the pipeline. “We kind of felt it was time,” said a government relations manager for Venoco. “The pipeline clearly is the mode of transportation that’s consistent with city and county policies.” In order to put pressure on the State Lands Commission to force Venoco to stop barging, the Board of Supervisors May 19 will consider sending a letter to the Commission, recommending “termination of the Ellwood Marine Terminal as soon as legally allowable, quickly followed by decommissioning of the terminal’s offshore mooring.” With or without the letter from the Board of Supervisors, the Commission’s staff, while recommending the Commission extend the barging lease until 2013 for legal reasons, has also recommended two conditions be attached to the extension. The conditions would require Venoco to either replace the single-hulled Barge Jovalan with a double-hulled barge, or obtain permits and move forward with construction of a pipeline. Whichever is chosen, it would have to be up and running within 18 months of the extension.
Source: http://www.thedailysound.com/News/051509oil

For more stories, see items **39** and **41**

[Return to top]

Chemical Industry Sector

3. *May 15, Louisville Courier-Journal* – (Kentucky) **Ammonia remains in building.** Emergency crews have not been able to get ammonia out of a storage company building two days after the deadly gas killed two workers. "Given the circumstances (and that) it's still not controlled, it's a major release," said the on-scene coordinator for the U.S. Environmental Protection Agency. Wednesday's leak at Louisville's American Cold Storage facility on Industry Road in the Algonquin neighborhood killed two maintenance workers. The on-scene coordinator said authorities had not yet determined the cause of the leak, or even if the leak had stopped. He said, however, that it appears it might have slowed. "The amount in there, if released, could still be a hazard to the community," said a spokesman for Louisville Fire and Rescue. A hint of ammonia could occasionally be smelled in the air. But the fire spokesman and the on-scene coordinator said authorities were monitoring the levels inside and outside the building, and there was no threat to the public.
Source: http://www.courier-journal.com/article/20090515/ZONE07/90515019/Ammonia+remains+in+building

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

4. *May 15, Associated Press* – (New York) **Valve problem shuts reactor in NYC suburbs.** The owners of New York's Indian Point nuclear power plant say one of their reactors has been shut down because of a valve problem. Entergy Nuclear says Indian Point 3 was safely turned off at 1:53 a.m. on May 15 with no release of radiation. It says there was a problem with a valve that controls the flow of water into a steam generator. The other reactor at the site in Buchanan, Indian Point 2, remained at full power. Buchanan is about 35 miles north of midtown Manhattan.
Source: http://www.wten.com/Global/story.asp?S=10368142
See also: http://www.nrc.gov/reading-rm/doc-collections/event-status/event/en.html#en45069

5. *May 14, U.S. Nuclear Regulatory Commission* – (Nebraska) **Fitness for duty involving a non-licensed supervisor.** A non-licensed employee supervisor at Cooper nuclear facility in Brownsville, Nebraska had a confirmed positive test for alcohol during a for-cause fitness-for-duty test. The employee's access to the plant has been temporarily suspended. The licensee notified the NRC Resident Inspector.
Source: http://www.nrc.gov/reading-rm/doc-collections/event-status/event/en.html#en45067

[Return to top]

Critical Manufacturing Sector

6. *May 13, KOLR 10 Springfield* – (Missouri) **Man killed in accident at Loren Cook Plant.** Police are investigating the apparent accidental death of an employee of the Loren Cook plant in Springfield on May 13. The police lieutenant says the 59-year old man was working with a piece of metal just after 1:00 p.m., when the metal came loose

from a piece of equipment and struck him in the head. Loren Cook manufactures large ventilation systems such as blowers, fans and circulators. Foul play is not suspected in the death.
Source: http://ozarksfirst.com/content/fulltext/?cid=148601

For another story, see item **37**

[Return to top]

Defense Industrial Base Sector

7. *May 14, Marine Log* – (National) **GAO: Navy shipbuilding programs don't use commercial yards' best practices.** The Government Accountability Office has completed a study of how U.S. Navy shipbuilding projects stack up against the best practices at leading commercial shipyards worldwide. And the answer would seem to be "not very well." The report is entitled "Best Practices: High Levels of Knowledge at Key Points Differentiate Commercial Shipbuilding from Navy Shipbuilding (GAO-09-322). GAO undertook the review in response to a mandate in the conference report accompanying the Defense Appropriations Act for FY 2008, Its object was to (1) identify key practices employed by leading commercial ship buyers and shipbuilders that ensure satisfactory cost, schedule, and ship performance; (2) determine the extent to which Navy shipbuilding programs employ these practices; and (3) evaluate how commercial and Navy business environments incentivize the use of best practices. To address these objectives, GAO visited leading commercial ship buyers and shipbuilders, reviewed its prior Navy work, and convened a panel of shipbuilding experts. In its summary GAO says that delivering ships on time and within budget are imperatives in commercial shipbuilding. To ensure design and construction of a ship can be executed as planned, commercial shipbuilders and buyers do not move forward until critical knowledge is attained. Before a contract is signed, a full understanding of the effort needed to design and construct the ship is reached, enabling the shipbuilder to sign a contract that fixes the price, delivery date, and ship performance parameters. To minimize risk, buyers and shipbuilders reuse previous designs to the extent possible and attain an in-depth understanding of new technologies included in the ship design. Before construction begins, shipbuilders complete key design phases that correspond with the completion of a three-dimensional product model. Final information on the systems that will be installed on the ship is needed to allow design work to proceed. During construction, buyers maintain a presence in the shipyard and at key suppliers to ensure the ship meets quality expectations and is delivered on schedule. "Navy programs often do not employ these best practices," notes GAO.
Source: http://www.marinelog.com/DOCS/NEWSMMIX/2009may00145.html

8. *May 13, Daily Tech* – (National) **U.S. Army looks forward to new generation of ground vehicles.** As the U.S. military still tries to adjust to fighting wars in Iraq and Afghanistan, the U.S. Army plans to develop new combat vehicles that will be specifically designed to fight insurgents who are implementing small arms fire and improvised explosive devices (IEDs). According to Army Chief of Staff, the new manned ground vehicle will be deployed overseas within five to seven years, as the

Army is just now beginning development of the new vehicles. In the 2010 military budget approved by the Pentagon, at least $26.23 billion will be spent on upgrading ground vehicles used by the Army and Marine Corps. The military has been highly criticized over lack of modernization of its vehicles that troops depend on when they go out on patrol. The military has been highly criticized over lack of modernization of its vehicles that troops depend on when they go out on patrol. It took years before the government began to re-enforce the armor on Humvees used by Marines and Army soldiers. To the dismay of private contractors working on the vehicles, the U.S. Defense Secretary was not overly impressed by the armor used to defend soldiers from IEDs. The FCS contract will now be re-written so the companies involved can still be involved in the project.
Source:
http://www.dailytech.com/US+Army+Looks+Forward+to+New+Generation+of+Ground+Vehicles/article15120c.htm

For another story, see item **37**

[Return to top]

Banking and Finance Sector

9. *May 15, New York Daily News* – (International) **NYPD breaks up identity theft ring in which 6,000 victims' credit wrecked, banks bilked out of $15M.** The New York City Police Department has crushed a sophisticated identity theft ring that wrecked the credit of 6,000 victims and bilked banks out of $15 million in bogus charges. The scam, which stretched from New York to Nigeria, is one of the largest operations of its kind dismantled by the NYPD, the police commissioner said on May 14. The thieves somehow managed to get their hands on thousands of credit cards legitimately issued in the victims' names, but intercepted them before they arrived at the proper destination. They then called the credit card companies, using a legal device called a SpoofCard to disguise their voice and phone number, to activate the credit cards. Once the companies fell for the ruse, the suspects used the cards for cash advances or to buy luxury items in Japan, Saudi Arabia and Dubai. In some cases, they even paid to boost the card's line of credit so they could go back for more cash. Once every penny was spent, the thieves recycled them as backup identification to open new credit accounts. The scam was discovered nearly two years ago when a Queens Realtor opened a package meant for one of his employees and found 60 credit cards, the type "normally issued in anticipation of a customer's card expiring," the police commissioner said. The NYPD traced those cards around the globe. During a 21-month investigation, cops used 80 phone taps to eavesdrop on more than 1 million calls, said the deputy chief, head of the special investigations division. Thirty-five suspects, mostly Nigerian immigrants in the city, were arrested and face charges of enterprise corruption, larceny and conspiracy.
Source: http://www.nydailynews.com/news/ny_crime/2009/05/15/2009-05-15_nypd_breaks_up_identity_theft_ring_in_which_6000_victims_credit_wrecked_banks_bi.html

10. *May 14, Bloomberg* – (National) **Regulators seek trace-like reporting for derivatives.**

U.S. regulators may impose the same price reporting and transparency requirements on over-the-counter derivatives that reduced bank profits by almost half in the corporate bond market when the Trace system was adopted seven years ago. “I think it is something we will look at very closely as a potential model,” the Securities and Exchange Chairwoman said on May 13 at a news conference in Washington, in which regulators laid out potential structural changes to improve policing of the $684 trillion OTC derivatives market. Trace, the bond-price reporting system of the Financial Industry Regulatory Authority, gives anyone with an Internet connection access to trading data for corporate bonds. The system, in full operation since February 2005, reduced the difference in prices that banks charge to buy and sell bonds by almost half. The Treasury Secretary, the chairwoman and the acting chairman of the Commodity Futures Trading Commission, called for increased oversight of over-the-counter derivatives to reduce risk to the financial system. Lax regulation contributed to the failures last year of Lehman Brothers Holdings Inc. and American International Group Inc., leading to the seizure of credit markets and causing more than $1.4 trillion in writedowns amid the worst financial crisis since the Great Depression.
Source: http://www.bloomberg.com/apps/news?pid=20601103&sid=a.e5Xpc90Q0Q&refer=news

11. *May 14, Reuters* – (National) **SEC proposes tougher investment adviser rules.** U.S. securities regulators proposed tougher rules designed to ensure that investment advisers are more accountable for their client’s assets in the wake of massive fraud. The Securities and Exchange Commission voted 5-0 on May 14 to propose that investment advisers who hold their client’s assets undergo a surprise exam once a year to make sure those assets exist. In most cases, investment advisers do not physically control their clients’ assets, and those assets are maintained with a broker-dealer or bank, also known as a qualified custodian. But the investment advisers who have “custody” of their customer’s assets either physically control or have the authority to withdraw their clients’ funds. The proposal is open for public comment and needs to be formally adopted before it becomes a rule.
Source: http://www.theusdaily.com/articles/viewarticle.jsp?id=745981&type=Business

12. *May 13, Atlanta Business Chronicle* – (Georgia) **Bremen man indicted for $7M in fraud.** A 43-year-old defendant was indicted on May 13 by a federal grand jury on charges of mail fraud, wire fraud, and money laundering in connection with an alleged $7 million fraud scheme. “In this latest chapter in the long book of investment fraud schemes, a man who lives in a small town in west Georgia allegedly persuaded investors from around the country that with his secret government contacts and other plans, he could make their money multiply into millions,” said a U.S. Attorney. “He will now be prosecuted in open court, where he is alleged to actually be just a thief who used lies to steal millions from his victims.” According to the U.S. Attorney, the charges and other information presented in court, starting in early 2006, the defendant allegedly promised investors that they would receive returns of between 40 percent and 150 percent on the money they placed in his “high yield” investment programs. The defendant claimed to own a bank, to have access to confidential and lucrative investment opportunities, or to

be a "special agent" of the Federal Reserve who the U.S. government authorized to stimulate the economy with cash injections. Between February 2006 and February 2007, 31 investors mailed or electronically transferred more than $7.4 million to the defendant, who allegedly spent the money on Haralson County real estate, vehicles, jewelry, fur coats, art, gambling trips to Las Vegas, and family cruises to Alaska, Hawaii and the Mediterranean. The defendant allegedly never invested any money, though he did make nominal payments to a few investors who persisted in asking to see their returns. The indictment includes charges of mail fraud, wire fraud, and money laundering.
Source: http://www.bizjournals.com/atlanta/stories/2009/05/11/daily61.html

[Return to top]

Transportation Sector

13. *May 15, Detroit Free Press* – (Michigan) **I-94 closed at Battle Creek over safety concerns.** A section of I-94 in southwest Michigan has been closed indefinitely after crews noticed that overpasses the state is rebuilding appear to have shifted, perhaps dangerously. Engineers for the Michigan Department of Transportation (MDOT) are regrouping May 15 to devise a way to shore up the bridges and reopen them possibly the week of May 18, an MDOT spokesman said May 14. The freeway was closed May 14 after workers notified MDOT of a visible shift indicating a deteriorated base supporting I-94 overpasses above Riverside Drive in Battle Creek. A joint on the eastbound bridge separated by at least six inches, he said. A project to replace bridges over Riverside in both directions of the freeway started about three weeks ago. Crews have removed half of each of the two bridges carrying I-94, leaving two lanes open each way. Engineers were examining the situation to determine whether it is safe to reopen the bridges or, in the worst case scenario, to keep them closed until replacements are built.
Source: http://www.freep.com/article/20090515/COL12/305150001/I-94+closed+at+Battle+Creek+over+safety+concerns

14. *May 14, Downtown Express* – (New York) **Emergency drill this Sunday.** Lower Manhattan residents should not be alarmed early May 17 when they see hundreds of emergency vehicles flooding the World Trade Center site. The sirens, street closures and more than 750 first responders will be a reaction to a pretend emergency, not a real one. The drill, starting at 8 a.m. May 17, will simulate the first 90 minutes to two hours following an explosion on a PATH train near the World Trade Center site. The Port Authority is leading the drill with participation from half a dozen other agencies and the local Community Emergency Response Team, whose members will don makeup to act as victims.
Source: http://www.downtownexpress.com/de_316/emergencydrill.html

For more stories, see items **1**, **2**, and **41**

[Return to top]

Postal and Shipping Sector

15. *May 14, Seattle Times* – (Washington) **Suspicious package in Shoreline turned out to be medicine.** The suspicious brown and white substance found on a package at the U.S. Post Office in Shoreline turned out to be a prescription medicine, according to a Shoreline Fire Department spokeswoman. Hazardous material experts from the Shoreline Fire Department and other agencies were called to the post office at 17233 15th Ave. N.E. around 10:45 a.m., the spokeswoman said.
Source: http://seattletimes.nwsource.com/html/localnews/2009220405_webshorelinehazmat14m.html

[Return to top]

Agriculture and Food Sector

16. *May 15, Associated Press* – (Iowa) **NE Iowa plant reopens after explosion.** A food processing plant in northeast Iowa that was damaged by an explosion and fire more than a year ago is back in business. Bay Valley Foods in New Hampton reopened on May 14 after being closed since February 2008 when a piece of equipment exploded. No one was injured in the accident and the cause was never determined. The plant produces powdered goods like nondairy coffee creamer and soup bases.
Source: http://www.kgan.com/template/inews_wire/wires.regional.ia/3fb87b9a-www.kgan.com.shtml

17. *May 14, Cattle Network* – (International) **NPPC: Novel flu strain not from Smithfield's Mexican hog farm.** Mexico's agriculture department said the influenza strain that now has infected almost 4,300 people in 33 countries did not originate from hogs at a Smithfield Foods operation that had been singled out by some as the source of the A-H1N1 flu virus. Test results released by the Mexican Ministry of Agriculture, Ranching, Rural Development, Fisheries and Food (SAGARPA) confirmed that the novel A-H1N1 virus was not in pigs at the Granjas Carroll de Mexico farm in Veracruz. The pigs also tested negative for other viruses. While the news was welcomed by the National Pork Producers Council, the organization said the damage to the U.S. pork industry from mislabeling the strain "swine" flu has been done.
Source: http://www.cattlenetwork.com/Content.asp?ContentID=315081

18. *May 14, U.S. Food Safety and Inspection Service* – (New Mexico) **New Mexico firm recalls red pork tamale products due to undeclared allergen.** Amigo's Mexican Food, Inc., a Deming, New Mexico establishment, is recalling approximately 4,594 pounds of red pork tamale products because they may contain an undeclared allergen, wheat, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced on May 14. Wheat is a known allergen, which is not declared on the label. The red pork tamale products were produced on various dates and were shipped to retail establishments in Arizona, New Mexico and Texas. The problem was discovered by FSIS during a routine product inspection. FSIS has received no reports of illness due to consumption of these products.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_020_2009_Release/index.asp

19. *May 14, U.S. Food Safety and Inspection Service* – (California) **California firm recalls frozen pork sausage products due to undeclared allergens.** Wayne Provision Co., a Vernon, California establishment, is recalling approximately 2,075 pounds of frozen pork sausage products because they may contain undeclared allergens, hydrolized soy and whey, the FSIS announced on May 14. Hydrolized soy and whey are known allergens, which are not declared on the label. Each label bears the establishment number "EST 4187" inside the U.S. Department of Agriculture mark of inspection. There are no package or case codes. The frozen pork sausage products were produced between August 2008 and April 2009, and were shipped to restaurants in southern California and the Las Vegas, Nevada area. The problem was discovered by FSIS during a routine product inspection. FSIS has received no reports of illness due to consumption of these products.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_021_2009_Release/index.asp

For another story, see item **3**

[Return to top]

Water Sector

20. *May 14, San Francisco Chronicle* – (California) **Feds raid Novato Sanitary District offices.** Agents with the U.S. Environmental Protection Agency (EPA) and the Federal Bureau of Investigation (FBI) raided the offices of the Novato Sanitary District on May 14, officials said. EPA officials said agents with its criminal investigation division and members of an agency task force served a search warrant at the district offices at 500 Davidson St. in Novato. Details of the investigation were not released. "Because this is an ongoing criminal investigation, we are not able to provide additional details regarding this case at this time," the EPA said. The district provides wastewater collection, treatment and disposal services to 60,000 residents in Novato. It also maintains a 200-mile sewer-collection system and two wastewater treatment plants.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/05/15/BAU317KMQH.DTL

21. *May 14, Edmonds Beacon* – (Washington) **Plant's alarm gives fire crew a workout.** The Edmonds Wastewater Treatment Plant is an industrial operation with a maze of buildings and tight spaces. On occasion, reduced staffing dictates use of the Worker Inactivity Alarm or "man-down alarm." If someone should become trapped or disabled, it is urgent that emergency crews respond immediately with rescue and medical equipment. On-site workers must reset a computer-based timer every hour. If they do not, the man-down alarm is programmed to activate and notify SnoCom 911 of the emergency. To prevent false alarms, a five-minute siren sounds at the treatment plant before the alarm signals SnoCom. Recently the Worker Inactivity Alarm alerted SnoCom that a rescue-tech response was imminent. The rescue crew arrived to find a full staff who believed the alarm must have malfunctioned. The Battalion Chief contacted SnoCom to determine why the alarm had rung there. SnoCom indicated the alarm had sounded as it was designed to do, with no problems at their end. Further investigation revealed that the Treatment Plant had recently conducted computer-battery

work, which was assumed to be the cause of the false alarm.
Source:
http://www.edmondsbeacon.com/index.php?option=com_content&view=article&id=1483:plants-alarm-gives-fire-crew-a-workout&catid=78&Itemid=186

22. *May 14, Water Technology Online* – (International) **Real-time monitoring device detects infrared 'colors': researcher.** A researcher at Tel Aviv University has developed a new system to monitor the safety of a building or community's water supply in real time, Web-based technology news service PhysOrg.com reported on May 14 from a Tel Aviv University news release. A professor of the university's School of Physics and Astronomy has modified special fibers developed in his university lab to detect "colors" not visible the human eye in the infrared spectrum that distinguish between pure and contaminated water. Connected to a commercial spectrometer, the fibers serve as sensors that can detect and notify authorities immediately if a contaminant has entered a water reservoir, water system, including pipelines, and water storage, such as for skyscrapers. According to the release, during lab experiments, the fiber-optic system detected contaminants such as pesticides in amounts well below the World Health Organization (WHO) safety threshold. Preliminary field experiments already have been completed at several European sites, and the results recently were reported in the Journal of Applied Spectroscopy. The special fiber sensors make it possible to monitor the quality of water in a remote location, such as a lake, a river or a pipeline, and detect trace amounts of contaminants in real time. According to the release, water management executives in Florida's Everglades and officials in Germany are among those who have expressed an interest in using the technology.
Source: http://watertechonline.com/news.asp?N_ID=71906

23. *May 13, Los Angeles Times* – (Alaska) **Alaska gold mine agrees to pay more than $800,000 for storm runoff.** The remote town of Nome, Alaska, has always depended on mining and has had to put up with the arsenic and mercury contamination that come along with it. But it got to be too much for many Nome residents last year when storm water thick with sediment pulsed into salmon-bearing streams. Now, operators of the Rock Creek Mine have agreed to pay $833,628 in civil penalties. The fine is one of the biggest ever assessed in the Northwest over Clean Water Act violations, said a compliance officer for the Environmental Protection Agency (EPA). The issue was ordinary silt allowed to wash into creeks as a result of heavy rainfall during construction in 2007 and 2008, hundreds of times above levels permitted under state water quality standards.
Source: http://latimesblogs.latimes.com/greenspace/2009/05/mine-pollution-alaska-fine-epa-nome.html

[Return to top]

Public Health and Healthcare Sector

24. *May 15, Associated Press* – (New York) **Another swine flu outbreak in NYC closes 3 schools.** Health investigators are trying to figure out why swine flu has spread erratically — moving quickly through a few schools but slowly elsewhere — after an outbreak

closed three more New York schools. The decision on Thursday to shutter the schools follows an outbreak that left an assistant principal in critical condition and sent hundreds of kids home with flu symptoms, in a flare-up of the virus that sent shock waves through the world last month. New York's mayor said four students and the assistant principal have documented cases of swine flu at a Queens middle school. More than 50 students have gone home sick with flulike symptoms, he said. At another middle school in Queens, 241 students were absent Thursday. Dozens more were sick at an elementary school. The Health Department said the assistant principal from the Susan B. Anthony middle school is on a ventilator, marking the most severe illness in the city from swine flu to date. The students who have fallen ill in this latest surge of illness appear to be experiencing mild symptoms, similar to routine flu.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5g4aIFEPab0nj0vrGzI3N09x0fbZwD986LB1O0

25. *May 14, Associated Press* – (Arizona) **1st Arizona swine flu-related death reported.** A woman in Arizona suffering from a lung condition has apparently become the fourth person with swine flu in the nation to die, authorities said Thursday. The Maricopa County Health Department reported that the woman in her late 40s died the week of May 4 of what appears to be complications of the new strain of influenza. Laboratory tests confirmed that the woman was infected with the flu strain. The federal Centers for Disease Control and Prevention is expected to add her to the official national tally on May 15, a health department spokeswoman said. Arizona's case would bring the number of swine flu-related deaths in the nation to four and put the worldwide death toll at 70.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5jQKNFu9iBzX02vBfajrRQpO_m1bQD986CCAG0

26. *May 14, Tech Herald* – (Maryland) **Insider might have walked off with 10,000 patient records.** In a letter sent to Maryland's Identity Theft Program, Johns Hopkins Hospital reported that a single insider might have exposed patient records, over 10,000 of them, after an internal investigation into identity theft discovered a common link with the victims and the hospital. Johns Hopkins started to receive reports in January from law enforcement, and some individuals themselves, that they were victims of identity theft. Johns Hopkins, with the aid of its corporate security department, local law enforcement, the USPS and Secret Service, narrowed the potential cause of the personal information leak to a single employee with access to the records in question. Since 31 of the confirmed 46 identity theft victims could be tied to the hospital, later tracked back to this employee, an indictment is expected soon. However, while the investigation narrowed down the source to a single person, "there is no absolute certainty, at this time, that she was the source of the information."
Source: http://www.thetechherald.com/article.php/200920/3681/Insider-might-have-walked-off-with-10-000-patient-records

[Return to top]

Government Facilities Sector

27. *May 15, Hartford Courant* – (Connecticut) **CCSU bomb threat at CCSU closes building.** The Connecticut state police bomb squad is investigating a bomb threat discovered Thursday morning in a building at Central Connecticut State University. The unspecified threat, written in graffiti, was discovered in the Robert C. Vance Academic Center early Thursday morning. A sweep of the building by the bomb squad on Thursday turned up nothing. But the squad is returning on the morning of May 15 to "double check," said a CCSU spokesman.
Source: http://www.courant.com/community/news/nb/hc-web-ccsu-bomb-scare-0515may16,0,6099637.story

28. *May 14, KHON 2 Honolulu* – (Hawaii) **Mysterious chemical odor forces evacuation of DMV building.** A mysterious odor in Kalihi sent two women to the hospital and forced the evacuation of more than a hundred people. The Honolulu Fire Department's HAZMAT team was called in to City Square at 7:45 a.m. on Thursday after workers complained of a noxious smell. Among the businesses affected was the city driver's licensing bureau where a line of people had been waiting just outside the door. It was bad enough for two area workers, who were taken by ambulance to a hospital. The state health department was also called in. In the meantime, businesses were told to leave the air conditioning off until the source is determined. The DMV decided it would be too hot to open so those who had been waiting in line for hours were forced to wait even longer. The city square facility will remain closed pending lab test results.
Source: http://www.khon2.com/news/local/story/Mysterious-Chemical-Order-Forces-Evacuation-of/joc9e0-_FU6A5F_Kz-DFoA.cspx

29. *May 14, Nextgov* – (National) **Defense networks breach reveals weaknesses in federal info security.** Tighter information security controls on government computers could have prevented the leak of confidential documents by a Pentagon official to a Chinese operative, according to members of the security industry. "There should be controls in place on these systems to limit copying of classified information, and logs should be reviewed regularly per employee activities on these systems," said the vice president of security awareness at Core Security Technologies and former senior data risk management specialist for the World Bank treasury security team. The deputy director of the U.S. Pacific Command's Washington liaison office was charged with espionage conspiracy, according to a May 13 press release from the Justice Department. The deputy director, who is on administrative leave from his job, is accused of providing an operative of the Chinese government with Defense Department documents and other information, some of which the deputy director obtained from classified online systems. The deputy director had Top Secret clearance and worked from both a classified and unclassified computer at his cubicle.
Source: http://www.nextgov.com/nextgov/ng_20090514_7707.php

30. *May 14, Associated Press* – (Texas) **San Antonio selected for new cyber security unit.** The Air Force has chosen a San Antonio base for a new cyber security and defense command. A Texas Senator said the Air Force Secretary chose Lackland Air Force Base

for the new cyber command. Air Force officials made no official announcement Thursday but were expected to do so on Friday. The cyber warfare command will employ about 400 people including the commander's staff and an around-the-clock operations center. The operations center will focus on defending Air Force networks against attacks and conduct some offensive operations. Lackland, which already conducts all Air Force basic training, beat out five other bases considered for the new cyber command.
Source: http://www.chron.com/disp/story.mpl/ap/tx/6424814.html

31. *May 14, Richmond Times Dispatch* – (Virginia) **Suspicious package prompts closure at city hall.** A suspicious package prompted the closure of part of City Hall in Richmond, Virginia, and a section of Ninth Street for about two hours on May 14, a spokesman for the Richmond Police department said. City Hall's entire A Level — including a parking deck, printing services and the mailroom where the package arrived — were evacuated from 2 p.m. to 4 p.m., the Richmond police spokeswoman said. The package was X-rayed, and because it was small it was decided there was no need to evacuate the entire building, the spokeswoman said. For about 2 and a half hours, Ninth Street was closed between Broad and Marshall streets, the spokeswoman said. The package was not addressed to anyone specific, and because it was heavily wrapped, it was removed to the state lab where it will be opened, the spokeswoman said.
Source: http://www.timesdispatch.com/rtd/news/local/article/CHALGAT14_20090514-174802/267714/

32. *May 12, Air Force Times* – (National) **Expert: Even routine work poses cyber-threat.** Simply doing business in today's online world puts sensitive Air Force information at risk of cyber attacks, despite the service's aggressive efforts to protect it, security experts say. Questions about the vulnerability of Defense Department data came up in April after the Wall Street Journal reported that cyber spies during the past two years stole reams of data about the F-35 Joint Strike Fighter program, which the Air Force leads. "The fact is, if you're attached to the World Wide Web you're vulnerable in some way," said a cyber and national security expert at the Heritage Foundation, a think tank based in Washington. Cyber attackers also can use the computer systems of government contractors to indirectly infiltrate the Defense Department network, said the director of federal business development for the cyber security company McAfee. It appears this is how the JSF program was breached. Once they infiltrate an unclassified system, hackers might use that access to get into classified systems, he said. Military agencies sometimes move information from an unclassified network to a classified network, and software inserted by hackers can inadvertently be moved with it.
Source: http://www.airforcetimes.com/news/2009/05/airforce_cyber_security_051209/

For more stories, see items **1** and **24**

[Return to top]

Emergency Services Sector

33. *May 15, Appleton Post-Crescent* – (Wisconsin) **Radio, paging equipment has its share of problems.** It will take an estimated $45 million to upgrade FoxComm, the regional emergency communications system, to meet new federal regulations and replace obsolete equipment, public safety officials in Wisconsin learned Thursday. FoxComm connected the Calumet, Outagamie and Winnebago county dispatch centers in 2002, and allowed them access to each other's records. It is, however, far from seamless. The system is actually a patchwork of different radio and paging systems. Some of the equipment is 20 years old, FoxComm's management information coordinator said. The systems is currently only capable of transmitting data at a speed of 19.2 kilobits per second, which is about three times slower than an Internet dial-up connection. Dispatchers cannot transmit a mug shot to officers without bogging down the system. Additionally, the system has so few channels that the Winnebago County SWAT team has to share a frequency with Waupaca County fire departments. The consortium began studying remedies for the problem in 2008. Consultants recommended upgrading to a system-wide 700 megahertz voice communications system and an 800 megahertz mobile data system. Transmitters and consoles would cost Calumet County about $5.1 million; Outagamie County $8.2 million and Winnebago County about $7.5 million. Radios would run an additional $1,500 to $2,500 each. The three counties would split an additional $3.2 million in infrastructure costs.
Source: http://www.postcrescent.com/article/20090515/APC0101/905150558/1979

For another story, see item **1**

[Return to top]

Information Technology

34. *May 15, Brand Republic* – (International) **Google blackout blamed on network 'traffic jam.'** Google blamed a network error for an "embarrassing" breakdown in service on May 14 as Gmail, search, YouTube, AdSense and Blogger all experienced outages, while Facebook suffered another phishing attack. Data routing issues caused several Google products to stop functioning on May 14, most notably Google's main search tool, before service was renewed an hour later. A systems error caused Google to direct web traffic through Asia, which created an internet traffic jam. As a result, about 14 percent of internet users experienced slow services and interruptions. A senior vice president for Google operations said: "Imagine if you were trying to fly from New York to San Francisco, but your plane was routed through an airport in Asia. And a bunch of other planes were sent that way too, so your flight was backed up and your journey took much longer than expected." Google apologized for the glitch, calling the incident "embarrassing" and said it would work diligently to avoid future breakdowns.
Source: http://www.brandrepublic.com/News/906101/Google-blackout-blamed-network-traffic-jam/

35. *May 14, CNET News* – (International) **Facebook members hit by another phishing scam.** In what is just the latest Facebook phishing scam, hackers on May 14 broke into accounts and sent e-mails to friends urging them to log on to fake Facebook sites, according to new reports and anecdotes from members. The social-networking site is in

the process of cleaning up from the hack and is blocking compromised accounts, Reuters reported. "Victims were directed to log back in to the site, but actually logged into the one controlled by the hackers, unwittingly giving away their passwords," Reuters said, adding that the fake domains include www.151.im, www.121.im and www.123.im. Facebook did not immediately respond to an e-mail seeking confirmation and information about the hack. The number of users affected remains unknown, but a Facebook spokesman told the New York Times it "is not widespread and is only impacting a small fraction of a percent of users." In addition to the scam, Facebook security made the news on May 14 in relation to upcoming plans for "verified apps" on the site. Under this program, Facebook will review developer apps for a $375 fee to make sure they fit security and transparency standards, and will award a graphic badge to apps that make the cut.
Source: http://news.cnet.com/8301-1009_3-10241573-83.html

36. *May 14, SC Magazine* – (International) **Scam sites increasingly masquerading as Facebook, MySpace.** Cybercriminals are tapping into the popularity of social networking to more effectively craft their scams. Increasingly, scam sites have domains that include the names Facebook, MySpace and Twitter, with no connection to the real sites. By using this tactic, called "domain-name cloning," cybercriminals are making their scam sites appear to be affiliated with these popular social networking sites. Websites with names such as unblock.facebookproxy.com, buy.viagra.twitter.1234.com or hotbabesofmyspace999.com often are phishing websites designed to lure users into handing over sensitive information or downloading malicious code, a security researcher for Websense Labs told SCMagazineUS.com on May 14. More than 200,000 phony copycat sites using in their URLs the terms Facebook, MySpace or Twitter have been identified. This problem may be heightened by a lack of user education, the researcher said. Because users are accustomed to looking at websites with the words Facebook, MySpace or Twitter in the URL, it is natural to think those sites are safe. Many of the domains are proxy avoidance sites that are used to evade traditional web filtering technology, Websense found when analyzing this threat. The researcher added that there are a few legitimate proxy avoidance sites, but the majority are operated by scammers who are up to no good and could be stealing usernames and passwords or infecting people with malware, he said.
Source: http://www.scmagazineus.com/Scam-sites-increasingly-masquerading-as-Facebook-MySpace/article/136868/

37. *May 14, CNET News* – (National) **HP laptop batteries recalled for overheating.** After two reports of flaming laptop batteries, the Consumer Product Safety Commission announced May 14 that Hewlett-Packard is voluntarily recalling 70,000 lithium-ion batteries that shipped with several models of its HP and Compaq laptops. The recall affects nine models of HP Pavilions, nine models of Compaq Presarios, two models of HPs, and one HP Compaq laptop model sold between August 2007 and March 2008. For the full list, see the CPSC's site. There were two separate reports of batteries that "overheated and ruptured, resulting in flames/fire that caused minor property damage" but no injuries, according to the CPSC report. HP is instructing consumers who may be part of the recall to remove the battery from their notebook and contact HP to find out if

theirs is affected. HP says it will provide a free replacement battery.
Source: http://news.cnet.com/8301-1001_3-10241137-92.html

38. *May 13, Communications Technology* – (International) **Botnets cause network headaches.** Internet service providers (ISPs) face a growing problem with the rise in botnets, malware that takes control of large numbers of computers. Over the last several months, the Conficker (sometimes called "Conflicker") botnet has infected more than 10 million machines by some estimates, dwarfing previous botnets by an order of magnitude. Security researchers have also discovered iBotnet, the first large scale Mac botnet, and Psyb0t, the first malware to take over Internet routers. These trends pose challenges for cable operators. One task is to alert customers without frightening them. In a March 31 post to the Comcast voices blog site, the Comcast Senior Director of Security and Privacy described Conficker and possible preventive actions. On the macro level, the biggest problem is the increase in Internet traffic associated with spam campaigns and distributed denial of service (DDoS) attacks, in which millions of compromised computers simultaneously send traffic to a Web site to disrupt service. Earlier this year, Time Warner Cable reported that its services had slowed because of a DDoS attack against its DNS servers. A cat-and-mouse game is playing out between security experts creating tools for finding viruses, Trojan horses and worms, and hackers finding new ways to circumvent them. Success lies in joining multiple elements rather than finding a single weakness. The massive spread of Conficker illustrates this shift in strategy.
Source: http://www.cable360.net/ct/news/ctreports/Botnets-Cause-Network-Headaches_35634.html

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

39. *May 15, Bangor Daily News* – (Maine) **60 mph winds cut power across state.** Strong winds on May 14 knocked out power to thousands of Mainers as gusts topping 60 mph brought down utility poles, trees, and limbs throughout the state. The blustery weather also was blamed for the loss of telephone service in some locations, including the Penobscot County Courthouse, which houses the county's administrative offices, the Sheriff's Department, the District Attorney's Office, the county jail, Superior Court and the Penobscot Regional Communications Center, among other things. Despite the problem with the county's business lines, which were still down late on May 14, 911 emergency services were not affected and continued to operate throughout the day, according to a news release sent to area media outlets. A Central Maine Power spokeswoman said wind-related power outages affected as many as 5,500 customers

during its peak between 12:30 and 1 p.m. Bangor Hydro-Electric Co. customers also lost power, with a total of nearly 4,500 as of 4:30 p.m., a company spokeswoman said.
Source: http://www.bangordailynews.com/detail/106082.html

40. *May 14, Courier-Life Publications* – (New York) **New effort to rein in cell phone towers.** New York City representatives have taken their first step toward curbing the proliferation of cell phone towers in the city's residential areas. A New York City Council member was a prime cosponsor of legislation which would require companies that apply to the city's Department of Buildings to install cell phone equipment on city buildings to send written notice to the community board and council member who represent the location prior to applying for the necessary permits. In addition, the legislation — which was introduced earlier this month — would require communications companies to attach identifying tags to their equipment, containing the permit number and a phone number to call in case there is any concern about the installation. It would also mandate the companies to make a good faith effort to locate their antennae and other equipment in nonresidential areas. Community notification is an important first step in controlling the placement of the antennae, said the City Council.
Source: http://www.yournabe.com/articles/2009/05/14/brooklyn_graphic/news/brooklyn_graphic_newsajdjiyc05132009.txt

For more stories, see items **34** and **38**

[Return to top]

Commercial Facilities Sector

See items **1** and **28**

[Return to top]

National Monuments & Icons Sector

Nothing to report

[Return to top]

Dams Sector

41. *May 15, Oregonian* – (Oregon) **Tug carrying gasoline hits section of the Dalles Dam; no leaks, Coast Guard says.** U.S. Coast Guard inspectors are on the Columbia River, dealing with an overnight accident on Friday that came when a tug pushing a barge alighted with part of the Dalles Dam. The incident, just after midnight, damaged the barge, which was carrying fuel. There were no reports of leakage or pollution and daylight should help determine whether the dam was also damaged, said a petty officer. During the investigation, commercial traffic has been temporarily halted, though

pleasure vessels are able to pass, she said.
Source:
http://www.oregonlive.com/news/index.ssf/2009/05/tug_carrying_gasoline_hits_sec.html

42. *May 14, HS Daily Wire* – (Oregon) **Oregon needs to raise Hagg Lake dam for fear of earthquakes.** In Oregon they expect the Big One — a massive earthquake — sometime in the next fifty years; one measure of preparation is to raise the height of dams so that earthquake-generated waves in the reservoirs behind the dams would not spill over and flood the neighboring territory of Washington County. This is because the earthquake prediction is affecting the cost of raising Scoggins Dam at Henry Hagg Lake, where most of the county plans to turn to for water over the next fifty years. A reporter for the Oregonian writes that a consultant's report will soon provide cost estimates for four new dam-raise options, said a spokesman for Clean Water Services, which is leading the project. Any of these options will be more expensive than originally expected, he said. Last spring, new studies led scientists to predict that a level-9 quake would occur in the Pacific Northwest sometime in the next 300 years, with a 10 to 14 percent chance it will happen in the next 50. The Bureau of Reclamation, which operates Scoggins Dam, began studying how it would hold up during such a quake and will have a report ready in October. A conceptual dam-raise design it had created earlier was inadequate, he said.
Source: http://www.hsdailywire.com/single.php?id=7980

43. *May 14, Emporia Gazette* – (Kansas) **Jam blocks Neosho River.** A massive logjam near the Hartford access ramp east of Hartford in Coffey County on the Neosho River formed recently. Officials have been told that the jam was caused by a cottonwood tree that is lodged under the bridge. The tree will not allow any other logs to pass under the bridge, creating a large logjam that is visible from the deck of the bridge and from the roadway east of Hartford. The Lyon County Emergency Management director said he heard of the logjam the morning of May 11. The jam is in Coffey County, but could affect the Hartford levee, the flow of the river, and the bridge. The property belongs to the U.S. Army Corps of Engineers and the county is working with that agency to see what can be done.
Source: http://www.emporiagazette.com/news/2009/may/14/jam_blocks_neosho_river/

[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 Website: http://www.dhs.gov/iaipdailyreport

Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
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