Homeland Security

Daily Open Source Infrastructure Report for 15 May 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- According to the Associated Press and Morning News, an empty 67,000-barrel gasoline tank undergoing repairs exploded Tuesday at a fuel storage facility owned by Teppco Partners in White County, Arkansas, killing three workers. (See item 2)
- Federal Computer Week reports that the Homeland Security Department's platform for sharing sensitive but unclassified data with state and local authorities was hacked recently, a DHS official has confirmed. The official said the U.S. Computer Emergency Readiness Team reported an intrusion into the Homeland Security Information Network in late March. (See item 21)

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 13, HS Daily Wire* – (National) **NERC approves strengthened cyber security standards.** Eight revised cyber security standards for the North American bulk power system were approved by the North American Electric Reliability Corp.'s (NERC)

independent Board of Trustees last week. The action represents the completion of phase one of NERC's cyber security standards revision work plan, which was launched in July 2008. Work continues on phase two of the revision plan, with version three standards already under development. The revised standards were passed by the electric industry last week with an 88 percent approval rating. The standards comprise approximately forty "good housekeeping" requirements designed to lay a solid foundation of sound security practices that, if properly implemented, will develop the capabilities needed to secure critical infrastructure from cyber security threats. Roughly half of those requirements were modified to clarify or strengthen the standards in this initial, expedited revisions phase. The revisions begin to address concerns raised by the Federal Energy Regulatory Commission in its Order No. 706, in which it conditionally approved the standards currently in effect. The revisions notably include the removal of the term "reasonable business judgment" from the standards. Entities found in violation of the standards can be fined up to $1 million per day, per violation in the United States, with other enforcement provisions in place throughout much of Canada. Audits for compliance with thirteen requirements in the cyber security standards currently in effect will begin on July 1, 2009.
Source: http://www.hsdailywire.com/single.php?id=7968
See also: http://www.nerc.com/news_pr.php?npr=308

2. *May 12, Associated Press and Morning News* – (Arkansas) **Three die in gasoline tank explosion.** An empty gasoline tank undergoing repairs exploded Tuesday at a fuel storage facility in White County, killing three workers, authorities said. The explosion occurred just before 2:30 p.m. at a storage facility owned by Teppco Partners, a Houston-based energy company, said a spokesman. The tank had been previously cleaned and workers were preparing to install a new gauge on it, he said. Three workers for an outside company contracted to do the repairs died in the explosion, said a spokesman for the Arkansas Department of Emergency Management. The Teppco spokesman said the company was in contact with local first responders and federal work safety investigators about the explosion. The Teppco spokesman said the tank was empty and not in service at the time of the explosion. He said the 67,000-barrel tank was being cleaned to prepare for new equipment to gauge the level of gasoline within the tank. He said it was not immediately clear whether the workers were inside or outside of the tank at the time of the explosion. A spokeswoman for the U.S. Occupational Safety and Health Administration in Dallas said federal investigators left for the explosion site Tuesday afternoon. She said she had no other details about the explosion. The Teppco facility, just east of U.S. 67 near McRae, stores diesel and unleaded gasoline for clients. The facility has five tanks with a capacity of 250,000 barrels. There appeared to be no release of fuel or fumes in the area surrounding the tank after the explosion, said a spokesman for the Arkansas Department of Environmental Quality. The explosion required no evacuations from the surrounding farmlands.
Source: http://www.nwaonline.net/articles/2009/05/12/news/051309argastankexp.txt

[Return to top]

Chemical Industry Sector

3. *May 14, Shreveport Times* – (Louisiana) **Hydrogen chloride tank leak being contained.** Area first responders are waiting for an environmental services company to arrive to contain and clean up after a hydrogen chloride leak on West Bert Kouns Industrial Loop near General Motors Boulevard. It was reported just before 5:30 a.m., with Louisiana state police first to be on the scene. They called the Caddo Parish sheriff's office, which around 7 a.m. had four units on the scene. The sheriff's spokeswoman said no evacuations have been ordered and that the leak apparently was from a tank mounted on a truck. Upon contact with moisture, hydrogen chloride turns into dangerously corrosive hydrochloric acid. Generally, the area in which the leak was reported is not populated save for industrial facilities.
Source: http://www.shreveporttimes.com/article/20090514/NEWS01/90514010

4. *May 13, KOVR 13 Sacramento* – (California) **Fairfield chemical plant fire danger lifted.** A Fairfield industrial plant that was evacuated May 13 after a chemical mixture turned into a potential fire hazard is no longer a hazard, according to the Fairfield Fire Department. One hundred employees of the Sun Pol resins factory were evacuated at 11:30 a.m. after two chemicals, used to make fertilizer, were combined and their temperature climbed to abnormal levels, creating a fire hazard. Buildings surrounding the factory were evacuated as a precaution. No homes were evacuated.
Source: http://cbs13.com/local/fairfield.fire.danger.2.1009106.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *May 14, Helsingin Sanomat* – (International) **TVO: Welding problems will not cause further delays to completion of Olkiluoto III.** The Finnish Radiation and Nuclear Safety Authority (STUK) has ordered the welding of the main circulation pipeline of Finland's fifth nuclear reactor, Olkiluoto III, to be suspended. Faults have once again been discovered in the welding seams, which are produced in France. STUK is requesting a clarification from the Finnish power company Teollisuuden Voima (TVO) and the French conglomerate Areva, which is constructing the installation, regarding the significance of the faults from the safety point of view. Only then can the welding work continue. According to a TVO project manager, the faults in question are only very minor surface blemishes that have no effect on the pipeline's strength or safety properties. He insists that the repairs will not cause further delays to the completion of Olkiluoto III. Areva discovered the faults in segments of the pipeline that are to be fitted between the evaporators and the reactor. Faults have been found in two welding joints. In all, there will be four joints. Microscopic fractures were discovered already in the first weld. STUK immediately demanded that Areva provide detailed plans on how to assess the cause of the faults, and how to proceed with the necessary further inspections. The second weld was flawless, but in the third weld completed at the beginning of May faults were again discovered. According to the STUK section head, the faults are almost identical to those in the first weld. He does not believe the observed faults are a result of a job poorly done. Rather, this is a question of factors related to the behavior of the material. He believes the investigation into the matter may take up to a couple of weeks.
Source:

http://www.hs.fi/english/article/TVO+Welding+problems+will+not+cause+further+delays+to+completion+of+Olkiluoto+III/1135245918243

6. *May 13, U.S. Nuclear Regulatory Commission* – (Washington) **Fitness for duty report.** A contractor supervisor at the Columbia Generating Station in Washington had a confirmed urine sample substitution on May 13. The employee's access to the plant has been terminated. The licensee has notified the NRC Resident Inspector.
Source: http://www.nrc.gov/reading-rm/doc-collections/event-status/event/en.html#en45065

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

7. *May 12, DarkReading* – (National) **Report: ATM/debit card fraud on the rise.** Credit card fraud may get most of the publicity when it comes to identity theft, but ATM and debit card theft is expected to grow 10 to 14 percent this year, according to a survey of financial institutions released May 12. It turns out the study was well-timed, too: Police officials in New York City reported on May 12 that a fraud ring had stolen $500,000 from hundreds of bank customers' accounts in the city using skimming devices affixed to ATM machines at Sovereign Bank branches in Staten Island. The skimmers read and stored their account information, and a rogue camera affixed to the machines captured victims' typing in their PIN numbers. They also used the information to clone the cards, according to published reports. Nearly 70 percent of the respondents to the survey, conducted by antifraud firm Actimize, said they had experienced an increase in ATM/debit card fraud claims in 2008 compared to 2007. Around 23 percent said those claims jumped by 5 to 9 percent; around 16 percent, by 10 to 14 percent; 17.5 percent, by 15 to 19 percent; nearly 9 percent, by 20 to 24 percent; 11 percent, by 25 to 49 percent; and 5 percent, by a whopping 50 to 74 percent. Half of the institutions had been hit with fraud complaints that came out of some of the major data breaches, with more than 30 percent saying they had seen fraud incidents as a result of the TJX hack, and 30 percent out of the Heartland Payment Systems hack. "It was interesting to confirm that not only are banking customers using ATM/debit card at risk, in general, because their data has been compromised and could be used for fraud, but it is being used for fraud," says the director of fraud solutions at Actimize.

Source: http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=217400522

8. *May 12, WOWT 6 Omaha* – (Nebraska) **Charges filed in Nebraska city broker scam.** Two former Nebraska City brokers face eight counts each of securities fraud. The two brokers were registered broker-dealer agents with Capital Growth Financial. They are accused of selling high-risk securities to roughly 150 Nebraskans without disclosing key risks or warnings. The total loss is estimated at more than $20 million. The securities were from two Florida-based companies, American Capital Corp. and Royal Palm Capital Group, Inc.; neither is still in business. An attorney for the investors says many of the victims sold their farms or small businesses to invest a considerable portion of that money to provide for retirement. Warrants have been issued for both brokers' arrests. If convicted, each count carries a penalty of up to five years in jail and/or a $10,000 fine.
Source: http://www.wowt.com/news/headlines/44786307.html

9. *May 12, Reuters* – (National) **Expanding FDIC borrowing could lower bank fees.** The U.S. Comptroller of the Currency said on May 12 an expansion of the Federal Deposit Insurance Corp's borrowing ability will help lower assessments charged to banks for deposit insurance. The Comptroller said he is happy with efforts in Congress to expand the FDIC's borrowing ability with the Treasury Department to $100 billion from $30 billion. The increased borrowing authority could allow the FDIC to forgo a special assessment on banks to replenish the U.S. deposit insurance fund. In February the FDIC proposed raising premiums and assessing a one-time fee of about 0.2 percentage points to raise about $15 billion to help replenish the U.S. deposit insurance fund, which has been steadily dwindling as banks fail. As banks try to shore up their capital, they have complained that they cannot afford to pay the assessment, which is scheduled for the third quarter. "Bank failures are likely to continue and the cost to the fund will likely increase," the Comptroller said at the conference of community bankers.
Source: http://uk.reuters.com/article/regulatoryNewsFinancialServicesAndRealEstate/idUKN1229801420090512?pageNumber=2&virtualBrandChannel=0

[Return to top]

Transportation Sector

10. *May 14, Akron Beacon Journal* – (Ohio) **Bomb report prompts Akron bus station evacuation.** Akron police are evacuating an area around the Downtown Transit Center on South Broadway because of a report of a bomb. South Broadway is also closed to traffic near the bus center. Deputies from the Summit County Sheriff's Office are on the scene and the bomb squad has been called in, said a lieutenant of the Akron Police Department. An off-duty deputy working at the Akron Metro Regional Transit Authority center called the threat in to the police, a dispatcher said.
Source: http://www.ohio.com/news/break_news/44978072.html

11. *May 13, Associated Press* – (Massachusetts) **Mass. transit authority banning driver**

cell phones. Massachusetts transportation officials announced May 12 they were immediately banning nearly all mass-transit drivers in Boston from using or even carrying cell phones or other personal digital assistants after a text-messaging trolley driver caused a crash last week that injured nearly 50 people. Metro Boston Transit Authority train, street car and bus drivers caught using the devices can be suspended for 30 days after the first offense, with a recommendation for discharge. Having the devices at work carries a 10-day suspension for the first offense, while a second offense carries a 30-day suspension, with a recommendation for discharge. The policy does not immediately apply to commuter rail engineers, who are employed by a different agency. The two-strike policy for carrying a device is aimed at leniency toward an operator who forgets he or she is carrying a phone, officials said.
Source: http://www.google.com/hostednews/ap/article/ALeqM5hm2-6gwMq2Tm0KBbo0AkT0MNOiiQD985F9401

12. *May 13, Chetek Alert* – (Wisconsin) **Emergency drill to simulate plane crash.** A large-scale emergency simulation drill will take place Sunday morning at the Chetek Municipal Airport. The drill will simulate an airplane crash into attendees of the annual air show in August. According to the Barron County Emergency Management director, local emergency personnel try to complete a large-scale drill once every other year, but a smaller, table-top drill is done once a month. "Our goal is to come up with continuity of operations between all emergency responders and have action plans for events that do take place in other communities," he says. The scenario has been in planning for nearly a year and will involve several local emergency responders-police, ambulance services, fire departments, hospitals, and local Boy Scouts. There should be nearly 350 people involved in the event. To make the drill as real as possible, there may be some roadblocks up around the airport area.
Source: http://www.zwire.com/site/news.cfm?newsid=20314446&BRD=1134&PAG=461&dept_id=150853&rfi=6

13. *May 13, Aviation Herald* – (New York) **Colgan DH8D at Buffalo on May 12th 2009, lost wheel on landing.** A Colgan Air de Havilland Dash 8-400, performing flight 9L-3268 from Newark, New Jersey to Buffalo, New York, had landed on Buffalo's runway 23 and was taxiing to the ramp via taxiway Alpha, when the tower queried the crew, whether they had lost a tire. After an affirmative reply from the crew emergency services inspected the taxiway and decided to also have a look onto the runway, then reported that fluid, possibly from hydraulics, was on the runway and a whole wheel had been located with debris around the intersections of runway 23, runway 32, and taxiway Alpha. Both runways were closed and runway 32 reopened about 10 minutes later.
Source: http://avherald.com/h?article=4198ce09&opt=0

For another story, see item **22**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

14. *May 12, U.S. Food and Drug Administration* – (New York) **Tofutti Brands Inc. announces precautionary recall of 12 pallets of Vanilla Cuties due to possible trace level milk contamination.** Tofutti Brands Inc. has completed a precautionary investigative recall of 12 pallets of its 8-Pack Vanilla Cuties mini sandwich frozen dessert novelties due to possible trace level milk contamination reported for a limited number of lots shipped which were produced in July of 2008. Vanilla Cuties are labeled as milk free. From early March to early April 2009, Tofutti Brands received telephone reports from 6 consumers who experienced skin rash symptoms after eating Vanilla Cuties produced at a minor production facility during three days in July of 2008. No illness or serious injury has been reported. The suspect product in question was identified as having been produced at only this one minor facility and the 12 pallets shipped from the suspect lots have been recalled. The bulk of these 12 pallets were recalled from the New York City metro area as well as from some distributed to the Midwest, New England, the Mid Atlantic Region, and California. Investigation and reports from distributors and store visits indicate that none of the suspect product remains in distribution and it is not currently being offered for sale. The suspect product in the above 12 pallets is identified by the labeled manufacturing facility code 360-300 which will appear on one of the two end flaps of the box of the Vanilla Cuties.
Source: http://www.fda.gov/oc/po/firmrecalls/tofutti05_09.html

15. *May 11, Tennessean* – (Tennessee) **StoneClear Springs plant engulfed by fire.** Firefighters were unable to save StoneClear Springs in Vanleer from being engulfed in flames the evening of May 10. The award-winning, locally owned water bottling company was burned to the ground after a fire broke about 8 p.m. on May 10. No one was injured in the blaze. Authorities are still investigating the incident to determine the cause of the fire. The 12,500-square-foot building was the workplace of six employees. The Vanleer Volunteer Fire Department, Cumberland Furnace Volunteer Fire Department, and Dickson County Fire & Rescue Squad responded to the incident. Fire fighters were able to contain the blaze to the main building, saving a small office building from the bulk of the conflagration.
Source:
http://www.tennessean.com/article/20090511/MICRO030401/90511015/StoneClear+Springs+plant+engulfed+by+fire+

[Return to top]

Water Sector

16. *May 14, WPXI 11Pittsburgh* – (Pennsylvania) **Water main break leaves gaping hole in Pittsburgh street.** A street on Pittsburgh's North Side will be closed on May 14 because of the hole left behind by a water main break. The Pittsburgh Water and Sewer

Authority said it discovered an 8-inch break in Chateau Street. That break caused a large sewer to collapse and created a hole in the street about 25 feet wide and 15 feet deep. Drivers will be detoured around the area, while crews make repairs. The street is expected to reopen around 6:00 p.m.
Source: http://www.wpxi.com/news/19458485/detail.html
See also: http://www.thepittsburghchannel.com/news/19455989/detail.html

[Return to top]

Public Health and Healthcare Sector

17. *May 14, Medical News Today* – (International) **WHO investigating claim that new H1N1 virus came from a lab.** The World Health Organization (WHO) is investigating a claim by an Australian scientist that the new H1N1 influenza virus, which was identified three weeks ago in Mexico and has now infected thousands of people in 33 countries around the world, came from a lab as a result of human error. The researcher, who has studied germ evolution for over 40 years and who worked on the early development of antiviral drugs for influenza, sent a three page study about his analysis to the WHO last weekend. He said that he also intends to publish the study. WHO's Assistant Director-General ad Interim for Health Security and Environment said in an interview that they were reviewing the paper and that the researcher was one of the first scientists to analyze the genetic structure of the new A (H1N1) virus. The researcher said the virus may have accidentally evolved in eggs that researchers used to make viruses for vaccine development. In a telephone interview reported by the Brisbane Times, he said he came to this conclusion after analyzing the origin of the virus from its genetic blueprint.
Source: http://www.medicalnewstoday.com/articles/149966.php

18. *May 13, Agence France-Presse* – (International) **Scientist arrested for smuggling vials used in Ebola research into U.S.** A Canadian scientist has been arrested for smuggling 22 vials stolen from Canada's National Microbiology Lab, used in Ebola and HIV research, into the United States, Canadian and U.S. officials said Wednesday. He was taken into custody while crossing the border from Manitoba province into North Dakota on May 5, said a spokeswoman for the Public Health Agency of Canada, which operates the lab. The scientist said in an affidavit he stole the vials, described as research vectors, from the Winnipeg lab on his last day of work there on January 21. He told U.S. border guards he was taking them to his new job with the National Institutes of Health at the Biodefense Research Laboratory in Bethesda, Maryland. U.S. authorities feared their contents could pose a terrorist threat. But tests later showed "they are not hazardous."
Source:
http://www.breitbart.com/article.php?id=CNG.1eb625e36e305c62ccc14e75288e023d.6f1&show_article=1

19. *May 13, USA Today* – (National) **USA ill-equipped for a swine flu pandemic, experts fear.** Though health officials say the swine flu outbreak appears relatively mild, some medical experts say the United States is unprepared in many ways to handle a severe pandemic. The world is "better prepared for an influenza pandemic than at any time in

history," said the director general of the World Health Organization, last week. Yet even before the flu outbreak, emergency rooms could barely handle all the patients coming through their doors, says the chair of Emory University's Department of Emergency Medicine in Atlanta. Emergency rooms have little "surge capacity," she says. In a crisis, she says, health workers might have to set up triage centers in public places, such as parking lots, to decide which patients are well enough to recuperate at home and which need medical attention. At Emory, she has even raised the idea of "drive-through" flu triage, with health workers performing quick assessments of heart rate, breathing, and mental status through the window. Other experts say the world could have trouble manufacturing enough vaccine. The director of the Center for Infectious Disease Research and Policy at the University of Minnesota commends the Federal Government for building a robust stockpile of antiviral drugs. Between national, state, and military supplies, the nation can treat 80 million people, or about 25 percent of the population, with antivirals, which can lessen the flu's severity if given within 48 hours of the appearance of symptoms and even prevent the flu if given to household members of flu patients. Considering that influenza often has an "attack rate" of 25 percent to 40 percent, those supplies may be enough, he says. But in a very severe outbreak, a person might need four times the usual amount of Tamiflu, leaving enough drugs for about 6 percent of the population, says a professor in infectious diseases at Johns Hopkins University School of Medicine. Antiviral medications might not work at all if the flu virus becomes resistant to it, the professor says.
Source: http://www.usatoday.com/news/health/2009-05-13-preparedflu_N.htm

20. *May 13, Search Engine Land* – (National) **Feeling sick? Google begins asking some searchers who look for illness-related terms.** Google began asking a small number of users who search for information about illnesses whether or not they have them on Wednesday. The experiment, which is part of a process that Google hopes will allow them to improve health-related search results plus perhaps build more trending tools like Google Flu, will run for at least the next few weeks. With Google Flu, Google correlates search data with reported outbreaks, to increase its confidence level. In cases where it lacks a correlating factor (are poison ivy cases even publicly reported?), understanding how many queries are really based on an actual illness over time might help with creating some future trending. But for the most part, this seems to have a much more immediate application as a way for Google to decide if certain results need more "cure" slanting. Assuming many people are suffering illnesses when they search for these queries, Google could conceivably shift its results to be more "cure" oriented.
Source: http://searchengineland.com/feeling-sick-google-begins-asking-19244

[Return to top]

Government Facilities Sector

21. *May 13, Federal Computer Week* – (National) **Information-sharing platform hacked.** The Homeland Security Department's platform for sharing sensitive but unclassified data with state and local authorities was hacked recently, a DHS official has confirmed. The intrusion into the Homeland Security Information Network (HSIN) was confirmed to Federal Computer Week by the chief information officer for DHS' Office of

Operations Coordination and Planning. The chief information officer said the U.S. Computer Emergency Readiness Team reported an intrusion into the system in late March. The initial hack was brief and limited, and it was followed by a more extensive hack in early April, the chief information officer said. The hacker or hackers gained access to the data by getting into the HSIN account of a federal employee or contractor, the chief information officer said. The bulk of the data obtained was federal, but some state information was also accessed, he added, and the organizations that owned the data and Congress were notified of the intrusion. The files that were accessed contained administrative data such as telephone numbers and e-mail addresses of state and federal employees. However, an investigation into the incidents has found that no Social Security numbers, driver's license numbers or financial data were obtained, the chief information officer said. Because HSIN is a sensitive but unclassified network "no information can be posted on HSIN that would cause anything more than minor damage to the homeland security mission," he said, adding that none of the accessed files dealt with the operations of either federal or state agencies that use HSIN.
Source: http://fcw.com/articles/2009/05/13/web-dhs-hsin-intrusion-hack.aspx?s=fcwdaily_140509

22. *May 12, Associated Press* – (Nebraska) **2 Neb. construction workers injured in fall.** Two construction workers have been injured in a fall at the Nebraska Air National Guard Base at Lincoln Airport. A Nebraska Air National Guard spokesman says the accident happened at about 9 a.m. Tuesday in a hangar at the air base. The spokesman says the two workers were about 20 feet off the ground inside a cage attached to a lift. The spokesman says the lift toppled, taking the two workers with it. The workers were taken to a Lincoln hospital with injuries. The extent of their injuries was not known. The spokesman says the contractor, the Nebraska National Guard, and the Lincoln Police Department are investigating the accident.
Source: http://www.kmeg14.com/Global/story.asp?S=10348026&nav=menu609_2_4

[Return to top]

Emergency Services Sector

Nothing to report

[Return to top]

Information Technology

23. *May 13, ZDNet News* – (International) **Viruses now penetrating deeper.** New malware variants have taken researchers by surprise by adapting new "stealth" methods to penetrate systems deeper so as to avoid detection, according to Kaspersky Lab. The antivirus company said in a video conference on May 13, a new variant of botnet, Sinowal, also known as Torpig, marks the first time cybercriminals have used such sophisticated methods. Kaspersky said Sinowal writes itself to the user's hard drive master boot record (MBR), the operating system's lowest level, and has been successful in avoiding detection by antivirus products. It said the worm has over the last month

been actively spreading through a number of methods including Web sites exploiting the Neosploit rootkit and a vulnerability in PDF software, Adobe Acrobat Reader. Kaspersky said new methods of infiltration have also rendered it nearly impossible for users to avoid infection, even if they are careful. Seemingly clean sites can also perform backend redirection to malware-ridden sites. The head of the virus lab for Kaspersky said Web malware authors have favored redirection exploits on Web apps and search fields, like iFrame attacks during 2008, compared to 2007 which saw more Trojan horses and droppers being used. The Web has also overtaken e-mail as the top transport medium for viruses, with the number of infected sites growing 300 percent in 2008, he said.
Source: http://news.zdnet.com/2100-9595_22-301551.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

24. *May 13, United Press International* – (California) **Fridge odor empties office, 7 hospitalized.** A refrigerator stench at a California AT&T call center in San Jose caused the building to be evacuated and seven people to be hospitalized with nausea, authorities said. The San Jose Fire Department said a hazmat team was sent to the office complex just before lunchtime May 12 and determined the odor was coming from an office mini-fridge, the San Jose Mercury News reported May 13. The stink caused seven people to be hospitalized with vomiting or nausea and 21 others were treated at the scene by paramedics. All 325 AT&T employees were evacuated from the building. A fire captain said he does not know what was causing the smell inside the refrigerator, but it smelled to him like rotting meat.
Source: http://www.upi.com/Odd_News/2009/05/13/Fridge-odor-empties-office-7-hospitalized/UPI-88511242253294/

25. *May 13, Associated Press* – (National) **FCC: Landline number move should take 1 day, not 4.** The Federal Communications Commission is telling landline phone companies that they now have to act faster when their subscribers want to move their phone number to a rival service. The commission voted May 12 to require companies to transfer, or "port," landline phone numbers within one business day, down from the current four-day requirement. Wireless numbers are currently ported within one day, and the commission noted that landline companies should be just as fast. The requirement takes effect in about a year. Landline numbers can be transferred to competing landline services, such as those from cable or Internet calling companies, or to cell phones.
Source: http://www.cellular-news.com/story/37452.php?source=rss

26. *May 13, CNET News* – (National) **Clearwire selects Cisco to help build 4G network.** Clearwire named networking equipment maker Cisco Systems as a key supplier to help it build its nationwide 4G wireless network, the companies announced May 12. As part of the new strategic partnership, Cisco will provide IP routers and other equipment to build Clearwire's network, which uses a technology called WiMax. Cisco will also develop some consumer devices that can be used on the network. Cisco would not provide specifics about the new products, but a Cisco representative said that these devices will be sold under the Linksys brand and are expected to be introduced later this year.
Source: http://news.cnet.com/8301-1035_3-10239541-94.html?tag=mncol;title

[Return to top]

Commercial Facilities Sector

See items **12** and **24**

[Return to top]

National Monuments & Icons Sector

27. *May 14, Denver Post* – (Colorado) **Black Canyon gets a scouring.** A whitewater torrent rushed over the Crystal Dam on Wednesday and coursed into Black Canyon of the Gunnison National Park. The release marked the end of a 36-year battle by the National Park Service to win an annual spring discharge from a series of dams upstream to cleanse and scour the river through the canyon. "This is the beginning of repairing and healing the park's ecosystem," said a Park Service hydrologist. Before the federal Bureau of Reclamation began gradually building up the flow last week, the Gunnison River was flowing about 1,000 cubic feet a second. Wednesday morning, the flow was about 7,500 cubic feet a second, or about 2 million gallons a minute. The stronger flow is intended to mimic natural spring runoff, removing sediment and algae and helping to break down riffles and whisk away vegetation encroaching on the riverbank, the hydrologist said. The natural flow of the Gunnison was blocked in the 1970s by the Aspinall Unit, a set of three dams built and run by the Bureau of Reclamation. The Park Service began trying to obtain a water right for the canyon in 1972. It was granted in late 2008.
Source: http://www.denverpost.com/news/ci_12365194

[Return to top]

Dams Sector

28. *May 14, KTVB 7 Boise* – (Idaho) **Flows along the Boise River increased.** Water flows along the Boise River were increased on May 14, and depending on temperatures, they could also increase next week. The Bureau of Reclamation and the U.S. Army Corps of Engineers say they need to increase the flows to make room in the Lucky Peak Reservoir for melting snowpack. And even though it is warming up, the two groups

discourage river recreation because of cold water temperatures, the high flow, and dangerous brush along the river banks.
Source: http://www.ktvb.com/news/localnews/stories/ktvbn-may1309-boise_river_flows.21ea795f.html

29. *May 13, Vernal Express* – (Utah) **Not in our backyard dam disaster drill. "**Hostages" filed out of the Flaming Gorge Dam Visitor Center with arms linked, providing a human shield for the terrorists who had taken over the visitor center during a mock disaster drill May 6. With a parking lot full of emergency response team command posts from all over Utah, the "terrorists" shot a Daggett County deputy, and set off an explosion, triggering the beginning of the day-long training exercise. Several terrorists took the volunteers hostage and barricaded themselves inside the visitor center. Although the terrorists succeeded in blowing up the dam with explosives and several hostages were shot, officials say the training exercise was a success. The drill involved the Bureau of Reclamation, FBI, Utah State Department of Public Safety, and Daggett County officers. A Blackhawk helicopter, a Highway Patrol helicopter, police boats and armored vehicles were used during the exercise. Training drills on the dam are required for Homeland Security. The aftermath of an attack on the Flaming Gorge Dam would be devastating, not only due to flooding below the dam, but also because of the water lost.
Source: http://www.vernal.com/pages/full_story?article-Not%20in%20our%20backyard-Dam%20Disaster%20Drill%20=&page_label=home_top_stories_news&id=2554387-Not+in+our+backyard-Dam+Disaster+Drill&widget=push&instance=home_news_right&open=&

[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

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.