Homeland Security

Daily Open Source Infrastructure Report for 19 May 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- A source close to the Times Square-bomber investigation said that the suspect had bigger, more destructive plans — other targets in New York and Connecticut. The source said that the suspect has told interrogators that if the Times Square bombing was successful, that he had four other locations to possibly attack: defense contractor Sikorsky in Connecticut and Rockefeller Center, Grand Central Terminal, and the World Financial Center across from Ground Zero in New York. (See item **16**)
- Students at Chamberlain High School in Tampa, Florida were greeted by extra security Tuesday morning, one day after a homemade acid bomb went off in a hallway and injured a student, putting the school on lockdown for several hours. Tampa police are providing additional security patrols Tuesday, saying they, along with school officials, are not taking the situation lightly. (See item **39**)

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 17, CBS and Associated Press* – (National) **Study: BP Refineries Produce 97% of Violations.** Two BP refineries in the U.S. account for 97 percent of "egregious willful" violations given by the Occupational Safety and Health Administration (OSHA), a Washington-based research group said. The study by the Center for Public Integrity said the violations were found in the last three years in BP's Texas City, Texas refinery and another plant in Toledo, Ohio. In 2005, 15 people were killed in an explosion at the Texas City refinery. The Deputy Assistant Secretary of Labor for OSHA said BP has a "systemic safety problem." He told The Associated Press that BP has not adequately addressed the issues, despite being fined more than $87 million. The Assistant Secretary of Labor for OSHA said similar problems are pervasive throughout the U.S. petroleum industry. Meanwhile, BP said Monday it was siphoning more than a fifth of the oil spewing into the Gulf of Mexico, but worries have escalated about the ooze reaching a major ocean current that could carry it through the Florida Keys and up the East Coast.
   Source: http://www.cbsnews.com/stories/2010/05/17/national/main6491769.shtml

2. *May 17, WAVY 10 Virginia* – (Virginia) **Cable stolen from Dominion Power.** Suffolk, Virginia, police are searching for the person or persons who stole several hundreds pounds of cable from a Dominion Virginia Power substation. A police spokesperson told WAVY.com the crime happened on either May 12 or May 13. The criminal(s) broke into the gated substation on Hosier Road and stole 300 pounds of Four Conductor Cable #6.
   Source: http://www.wavy.com/dpp/news/local_news/suffolk/cable-stolen-from-dominion-power-

3. *May 17, KIAH 39 Houston* – (Texas) **Plant fire, explosion hits Pasadena.** An explosion and huge cloud of black smoke rocked the Southeast Houston area Monday, May 17. While the all clear has been signaled, questions still remain about what caused the blast at Lyondell Basell. The plant handles plastic, chemicals, and refining. A thorough investigation has been launched by the plant to determine what caused this fire. The good news for the company — all personnel was accounted for after the fire. The fire started at 2:30 p.m. inside one of the crude distillation units at the plant. An hour later, firefighters came to the scene to extinguish the blaze. "This is a unit that takes the crude oil into the refinery and upgrades it into gasoline and other products," said a Lyondell Basell spokesperson. Lyondell Basell said that employees were not doing anything out of the ordinary before the fire took place. There were two firefighters treated from heat exhaustion. There were no other reports of any injuries. "We do have response teams that are in the field that are continuing to put water into the area to ensure that the fire remains out," the spokesperson said. "There is liquid on the ground." The crude distillation until has been shut down, and will remain that way until Lyondell Basell has a better understanding of what exactly occurred. "We'll focus on the business recovery aspects of this," he said. Lyondell Basell industries is one of the world's largest chemical and fuel makers.
   Source: http://www.39online.com/news/local/kiah-plant-fire-pasadena-story,0,6044681.story

[Return to top]

Chemical Industry Sector

4. *May 17, U.S. Environmental Protection Agency* – (National) **EPA adds more than 6,300 chemicals and 3,800 chemical facilities to public database.** The U.S. Environmental Protection Agency (EPA) has added more than 6,300 chemicals and 3,800 chemical facilities regulated under the Toxic Substances Control Act (TSCA) to a public database called Envirofacts. The Envirofacts database is EPA's single point of access on the Internet for information about environmental activities that may affect air, water and land in the U.S and provides tools for analyzing the data. It includes facility name and address information, aerial image of the facility and surrounding area, map location of the facility, and links to other EPA information on the facility, such as EPA's inspection and compliance reports that are available through the Enforcement Compliance History Online (ECHO) database. EPA is also adding historic facility information for another 2,500 facilities. EPA has conducted a series of aggressive efforts to increase the public's access to chemical information including reducing confidentiality claims by industry, and making the public portion of the TSCA inventory available free of charge on the agency's Web site. EPA intends to take additional actions in the months ahead to further increase the amount of information available to the public.
   Source:
   http://yosemite.epa.gov/OPA/ADMPRESS.NSF/d0cf6618525a9efb85257359003fb69d/b6e361b5203809948525772600 4e5a98!OpenDocument

For another story, see item **3**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

5. *May 18, Associated Press* – (North Carolina) **Nuke regulators talk to neighbors of NC plant.** The federal agency that oversees the country's nuclear power plants wants to hear from neighbors of a North Carolina operator. The Nuclear Regulatory Commission (NRC) has scheduled a meeting for Tuesday to talk about the agency's assessment of safety performance last year at the Shearon Harris nuclear power plant 20 miles southwest of Raleigh. The evening meeting in Apex includes a question-and-answer session. NRC staffers said the Harris plant operated safely in 2009, and there were no inspection results leading the agency to increase its degree of oversight. The plant is owned by Raleigh-based utility Progress Energy.
   Source: http://www.charlotteobserver.com/2010/05/18/1442800/nuke-regulators-talk-to-neighbors.html

6. *May 17, Las Vegas Sun* – (Nevada) **Nevada files motion for Yucca application withdrawal.** The state of Nevada filed a motion Monday with the Nuclear Regulatory Commission, asking it to approve the application of the Department of Energy (DOE)

to pull out of Yucca Mountain. The regulatory commission will hold hearings in Las Vegas on June 3-4 on the application to withdraw. The petition, signed by a Texas attorney says the regulatory commission "cannot second-guess an applicant's decision to withdraw a license application." The attorney said the withdrawal must be granted with prejudice so that it could never be filed again. This would prevent the DOE from resubmitting it in the future. In announcing its decision to pull out, the DOE said "developing the Yucca Mountain repository is not a workable option and that the nation needs a different solution for nuclear waste disposal." It said it was ending its agreement with the Office of Civilian Radioactive Waste Management.
Source: http://www.lasvegassun.com/news/2010/may/17/nevada-files-motion-yucca-mountain-withdrawal/

7. *May 17, Bloomberg* – (National) **Miniature nuclear plants seek approval to work in U.S.** Manufacturers of refrigerator-sized nuclear reactors will seek approval from U.S. authorities within a year to help supply the world's growing electricity demand. The chief executive officer of Hyperion Power Generation Inc., intends to apply for a license "within a year" for plants that would power a small factory or town too remote for traditional utility grid connections. The Santa Fe, New Mexico-based company and Japan's Toshiba Corp. are vying for a head start over reactor makers General Electric Co. and Areva SA in downsizing nuclear technology, and aim to submit license applications in the next year to U.S. regulators. They are seeking to tap a market that has generated about $135 billion in pending orders for large nuclear plants. "We're building iPhones when the nuclear industry has traditionally built mainframe computers," said the CEO. Hyperion has more than 150 purchase commitments from customers such as mining and telecom companies, provided its technology gets licensed for operation, he said. A generation after the Chernobyl and Three Mile Island accidents wiped reactor construction off the agenda of many governments, developers are pressing ahead with designs to satisfy demand for power that doesn't pollute the skies.
Source:
http://www.bloomberg.com/apps/news?pid=20601109&sid=aNWxvJD2xhZ8&pos=14

8. *May 17, Las Vegas Review-Journal* – (National) **UNLV researchers seeking ways to reprocess nuclear fuel.** A team of radioÂchemistry researchers routinely goes about its work at the University of Nevada, Las Vegas in hopes that someday they really will know what they have done and that it will make a difference. Led by an associate professor, the team is exploring new ways to reprocess used nuclear fuel so it can be used again, or recycled, instead of sitting in water pools or dry casks at nuclear power reactor sites awaiting disposal in a repository such as what Energy Department scientists had envisioned for Yucca Mountain, 100 miles northwest of Las Vegas. With that motto from the father of modern physics on their minds, the UNLV scientists work to solve problems of reprocessing, which have so far proved elusive. If reprocessing questions are answered during the next few decades or sooner, scientists of the future might be able to develop reactors that are better than the ones countries such as France and Japan are using today. This will enable them to squeeze more energy out of the uranium and plutonium in used fuels and leave relatively less for disposal.

Source: http://www.lvrj.com/news/unlv-researchers-seeking-ways-to-reprocess-nuclear-fuel-93914284.html

[Return to top]

Critical Manufacturing Sector

9. *May 18, Reliable Plant Magazine* – (Connecticut) **Metal finishing plant cited for 45 safety and health hazards.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has cited Har-Conn Chrome Company Inc. for 45 alleged serious violations of safety and health standards at its West Hartford, Connecticut, metal-finishing plant. "The conditions found at this workplace exposed employees to a variety of potential hazards including electrocution, fire, falls, lacerations and exposure to toxic substances," said OSHA's area director in Hartford. "For the safety and health of its workers, this employer must address these hazards completely, effectively and on an ongoing basis to prevent their recurrence." OSHA's inspection identified numerous electrical hazards, including exposed live parts, damaged or misused electrical equipment and wiring, blocked access to electrical wiring and the use of unapproved wiring; unguarded saws, fans and grinders; improper transfer of flammable liquids; improper storage of compressed gas cylinders; confined space hazards; untrained forklift operators; lack of personal protective equipment; and lack of emergency eyewashes. Additional hazards included failing to: determine workers' exposure levels to hexavalent chromium; provide annual medical surveillance and training to exposed workers; establish a regulated work area and ensure contaminated protective clothing remained in the work area; conduct cadmium exposure sampling. OSHA has proposed a total of $77,500 in fines. OSHA issues serious citations when death or serious physical harm is likely to result from hazards about which the employer knew or should have known.
Source: http://www.reliableplant.com/Read/24619/Metal-finishing-plant-safety-hazards

10. *May 17, Consumer Affairs* – (National) **2010 Chrysler, Dodge, Jeep models recalled.** Chrysler is recalling about 40,000 Chrysler, Dodge and Jeep models from the 2010 year. The vehicles may have a defective ignition switch that would allow the key to be removed prior to placing the shifter in the "park" position. This could lead to unintended vehicle movement. The affected models are: 2010 Chrysler 300, 2010 Dodge Challenger, 2010 Dodge Charger, 2010 Dodge Ram, 2010 Jeep Commander, and 2010 Jeep Grand Cherokee. Dealers will inspect the ignition module and replace defective units free of charge when the recall begins in July 2010.
Source: http://www.consumeraffairs.com/recalls04/2010/chrysler_ignition.html

11. *May 17, Consumer Affairs* – (National) **2010 Subaru Legacy, Outback recalled.** Subaru is recalling nearly 30,000 Legacy and Outback vehicles from the 2010 model year. The CVT cooler hose can split, resulting in a fluid leak, which could cause the car to come to an unexpected stop. Subaru will notify owners and dealers will replace any defective hoses free of charge.
Source: http://www.consumeraffairs.com/recalls04/2010/2010_subaru.html

12. *May 17, Consumer Affairs* – (National) **2010 Nissan Altimas recalled.** Nissan is recalling a small number of 2010 Altimas because some structural welds may be out of specification, which could affect vehicle crash performance. Dealers will inspect the vehicles and, if necessary, repair them free of charge. The affected units were assembled from April 7, 2010 through April 13, 2010.
Source: http://www.consumeraffairs.com/recalls04/2010/2010_altima.html

13. *May 17, Consumer Affairs* – (National) **2008-2010 Volvo XC70 recalled.** Volvo is recalling certain XC70 models from the 2008 through 2010 model years. The affected models contain incorrect tire inflation information. Dealers will inspect the vehicles and, if necessary, install a new tire and loading information label and tire-pressure management software. The owners manual will also be updated.
Source: http://www.consumeraffairs.com/recalls04/2010/volvo_xc70.html

For another story, see item 7

[Return to top]

Defense Industrial Base Sector

14. *May 18, Aviation Week* – (International) **U.S. industry hit by LCA clearance problem.** India is turning to Europe for support of the naval version of its Light Combat Aircraft (LCA) after its initial choice of the U.S. was stymied by an inability to gain the requisite approvals from Washington. India selected Lockheed Martin as the winner of a bid for consultancy work on its naval LCA, but failure to secure U.S. State Department licensing approvals has resulted in EADS being in negotiation for the work. This is not the first time regulatory issues have tripped up U.S. ambitions in India. In April 2009 EADS picked up flight-test work on the air force LCA as a result of Boeing being forced to withdraw. The U.S. manufacturer had been tapped for the project in 2008, but an inability to gain the required approvals from the U.S. administration forced it to pull its bid. The naval LCA is being designed for short take-off, but arrested recovery (Stobar), with a first flight of the naval variant by December. Neither EADS nor Lockheed are willing to comment beyond general statements. The U.S. company said it "continues to work with the U.S. government to support the LCA program. EADS, beyond confirming it has a consultancy contract (for the air force aircraft), said "both sides have agreed they will not disclose any details."
Source:
http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/asd/2010/05/18/01.xml

15. *May 18, Global Security Newswire* – (National) **Capabilities of U.S. missile interceptor questioned.** A new analysis of the U.S. Standard Missile 3, which rests at the center of the U.S. President's plan for Europe-based missile defenses, determined that the interceptor appears much less successful at destroying incoming warheads than was previously asserted, the New York Times reported. The new assessment by physicists and missile-defense skeptics revisited the results of 10 missile-interception

tests that occurred between 2002 and 2009 and had previously been announced as successful. The study concluded that the ship-based SM-3 was actually truly successful in no more than two tests — an achievement rate of only 10 to 20 percent compared to the 84 percent overall success rate touted by the Defense Department in its own earlier analysis of the interceptor. The authors judged a true success to be destroying the warhead on the incoming missile, not merely disrupting its flight path by hitting the much-larger body of the rocket. In most of the tests, the SM-3 was successful at the latter but not the former, they said. This is troublesome because a nuclear-armed missile could still explode after being knocked off course. In a real-life situation, "the warhead would have not been destroyed, but would have continued toward the target," the physicists concluded. The Pentagon has asserted that the SM-3 should both intercept and destroy the warhead on a missile.
Source: http://www.globalsecuritynewswire.org/gsn/nw_20100518_3770.php

16. *May 18, WNYW 5 New York* – (Connecticut; New York) **Source: Faisal Shahzad had bigger targets.** A source close to the Times Square-bomber investigation said that the suspect had bigger, more destructive plans — other targets in New York and Connecticut. The source said that the suspect has told interrogators that if the Times Square bombing was successful, that he had four other locations to possibly attack. If the bomb inside the Nissan Pathfinder in Times Square went off as planned, a source said that the bomber said he was taking aim at four other high-profile targets: Connecticut-based defense contractor Sikorsky, Rockefeller Center, Grand Central Terminal, and the World Financial Center across from Ground Zero. Sikorsky manufacturers helicopters for the U.S. military, including the Blackhawk. Headquartered in Stratford, Sikorsky also has facilities in Shelton and Bridgeport — the same two cities where the bomber has lived.
Source: http://www.myfoxny.com/dpp/news/international/source-faisal-shahzad-had-bigger-targets-20100517

17. *May 17, Kansas City Star* – (Missouri) **GSA official wants Bannister cancer investigation expanded.** The top official of Kansas City's General Services Administration wants a cancer investigation to be expanded to include not only current workers but former workers at the Bannister Federal Complex. The National Institute of Occupational Safety and Health began a review of current employees who have experienced cancer recently. But the newly appointed regional administrator of GSA said Monday most questions about worker illnesses are coming from former employees. GSA occupies about 45 percent of the Bannister complex in Kansas City, Missouri. Honeywell leases the rest for making nuclear bomb parts.
Source: http://www.kansascity.com/2010/05/17/1952742/gsa-official-wants-bannister-cancer.html

[Return to top]

Banking and Finance Sector

18. *May 17, Krebs on Security* – (International) **Teach a man to phish...** Phishing may not be the most sophisticated form of cyber crime, but it can be a lucrative trade for those who decide to make it their day jobs. Indeed, data secretly collected from an international phishing operation over 18 months suggests that criminals who pursue a career in phishing can reap millions of dollars a year, even if they only manage to snag just a few victims per scam. Phishers often set up their fraudulent sites using ready-made "phish kits" — collections of HTML, text and images that mimic the content found at major banks and e-commerce sites. Typically, phishers stitch the kits into the fabric of hacked, legitimate sites, which they then outfit with a "backdoor" that allows them to get back into the site at any time. About a year and a half ago, investigators at Charleston, South Carolina based PhishLabs found that one particular backdoor that showed up time and again in phishing attacks referenced an image at a domain name that was about to expire. When that domain finally came up for grabs, PhishLabs registered it, hoping that they could use it to keep tabs on new phishing sites being set up with the same kit. The trick worked: PhishLabs collected data on visits to the site for roughly 15 months, and tracked some 1,767 Web sites that were hacked and seeded with the phishing kit that tried to pull content from the domain that PhishLabs had scooped up. When PhishLabs plotted the guy's daily online activity, the resulting graph displayed like a bell curve showing the sort of hourly workload a person would typically see in a regular 9-5 job, a researcher said. "In the middle of the day he's super busy, and in the mornings and evenings he's not. So this is very much his day job."
Source: http://krebsonsecurity.com/2010/05/teach-a-man-to-phish/

[Return to top]

Transportation Sector

19. *May 17, Associated Press* – (Virginia) **Small fire breaks out at Reagan airport restaurant.** Airport officials said a small fire at a Reagan National Airport terminal has caused some minor flight delays. A Metropolitan Washington Airports Authority spokeswoman said the fire broke out inside a McDonald's restaurant past the security checkpoint about 3 p.m. Monday. The spokeswoman said the airport fire department extinguished it within a few minutes. She said she doesn't know what caused the fire. The spokeswoman said people were moved to the other side of the terminal, but there were no evacuations. She said some flights leaving from gates near the restaurant had minor delays. No one was injured.
Source: http://wtop.com/?nid=25&sid=1959182

20. *May 17, StarTribune* – (Minnesota) **Delta flight heads back to Japan to kick off disruptive passengers.** Nearly 400 people aboard a Delta flight headed to Minneapolis on Monday wound up returning to Japan, where two disruptive passengers were removed by Japanese authorities. A Delta spokeswoman said the two passengers refused to cooperate with the crew aboard Flight 620 and were being questioned by Japanese authorities. She couldn't identify the passengers because of privacy concerns and didn't have details about the unruly behavior. The crew was three hours into what usually is about a 13-hour flight when it turned the plane around, the spokeswoman

said. The Boeing 747 carried 383 passengers and 14 crew members. The spokeswoman said the airline will run an extra flight from Japan to Minneapolis on Tuesday to accommodate those stranded by Monday's canceled flight.
Source:
http://www.startribune.com/local/94014419.html?elr=KArks:DCiUHc3E7_V_nDaycUiD3aPc:_Yyc:aUU

21. *May 17, WABC 7 New York* – (New York) **Investigation into alleged TSA thefts at JFK airport.** They are the backbone of airport security. The TSA screeners who watch to make sure nothing dangerous is put into travel bags, but at John F. Kennedy International Airport (JFK), it's what's being taken out that has some passengers upset. Dozens of travelers have had valuables stolen while going through TSA screening checkpoints at JFK in just the past 8 months. Port Authority Police records show the thefts involve expensive bracelets worth thousands of dollars, high-end watches, iPhones, even prescription medications. In February, a woman's $3,000 watch disappeared from one of the bins as it went through X-ray at a JFK checkpoint. She strongly suspects a TSA agent took it, and she finds that deeply disturbing. "They're stealing from us, this is a national security issue. What if somebody gives them $10,000 and says 'look the other way, let's put this bag through?' " said the woman. In the last three years, four TSA checkpoint screeners at JFK have been fired for theft while only one has been fired at Newark Airport, and 1 at LaGuardia Airport. Last July, two Kennedy Airport screeners got caught red-handed swiping a cell phone and laptop from luggage during a TSA integrity sting. The Port Authority said there have been 51 cases of theft at TSA check points at JFK in the last two years. Police sources said the number is probably much higher, especially since many times, the thefts are never reported.
Source: http://abclocal.go.com/wabc/story?section=news/investigators&id=7447038

22. *May 17, Associated Press* – (New York) **Amtrak fuel spill being investigated in central NY.** Officials said a fuel tank on an Amtrak passenger train was punctured when it was struck buy an object in central New York, shutting down rail service for several hours. About 500 gallons of diesel fuel spilled from the westbound Amtrak locomotive after Sunday afternoon's accident in Whitestown, just west of Utica. An Amtrak official said the object came from a CSX Corp. work train on an adjacent track. Some of the approximately 100 passengers on the Amtrak train say they heard a loud noise and saw flames before the train was stopped and they were evacuated. No one was injured. Buses transported passengers to the Utica station to await other trains. It was unclear what had struck the Amtrak train. CSX officials said the company is investigating the accident.
Source: http://www.wten.com/Global/story.asp?S=12494474

23. *May 15, Houston Chronicle* – (Texas) **Storm wreaks havoc throughout Houston area.** Heavy rainfall Friday evening caused a wreck that shut down a major Houston highway for hours. The rainfall also led to flight cancellations and delays at both of Houston's major airports, power failures and a tunnel collapse in Fort Bend County. At the Fort Bend County Sheriff's Office, a road over a tunnel being built to transport

inmates from the justice center to the jail collapsed due to the heavy rain, officials said. No one was injured. At CenterPoint, officials said about 13,000 customers were without power because of the storm.
Source: http://www.chron.com/disp/story.mpl/metropolitan/7006011.html

For more stories, see items **16** and **58**

[Return to top]

Postal and Shipping Sector

24. *May 17, KCRA 3 Sacramento* – (National) **Man pleads guilty to anthrax threats.** A transient pleaded guilty Monday to sending anthrax-hoax letters, threatening the President and failing to register as a sex offender. According to a plea agreement, the 62-year-old suspect admitted that he sent hoax mailings addressed to Social Security Administration offices that contained a white powdery substance and an index card with the words "you stole my money" and "die." As a result of the mailing to the New York Social Security office, 25 to 30 employees were evacuated, and four were quarantined, federal officials said. The suspect also admitted to making threats against the President. The letter to the President contained a white powder to simulate anthrax, prosecutors said. The suspect also admitted that, by virtue of a conviction in Texas, he was required to register as a sex offender in California and that he did not do so. He is scheduled to be sentenced August 2. The suspect faces a maximum statutory penalty of five years in prison and a $250,000 fine for sending hoax mailings and making threats to the president. For failing to register as a sex offender, he faces a maximum of 10 years in prison and a $250,000 fine.
Source: http://www.kcra.com/mostpopular/23583695/detail.html

[Return to top]

Agriculture and Food Sector

25. *May 18, Associated Press* – (Colorado) **Colo. rancher accused of neglect may lose cattle.** A Park County, Colorado rancher faces having his cattle taken from him if he is found to be an unfit owner. State officials said they seized 300 cattle from the man's ranch near Hartsel after they found 100 dead animals and other severely malnourished cattle. A hearing was slated for 9 a.m. May 18 in Park County District Court to determine if the rancher is an unfit owner. The Colorado Department of Agriculture said the Park County sheriff's department is conducting a criminal investigation. The department said there are an estimated 800 to 1,400 cattle on the ranch. The rancher told The Denver Post that he is good to his livestock and believes the investigation stems from an ongoing land dispute with nearby residents.
Source:
http://cbs4denver.com/wireapnewsco/Colorado.rancher.accused.2.1700159.html

26. *May 18, KMTR 16 Springfield* – (Oregon) **Cross-contamination likely in Roseburg.** Douglas County Public Health (DCPH) department officials said cross contamination is likely what caused 30 people to contract salmonella after eating at the Los Dos Amigos restaurant on Jackson Street in downtown Roseburg, Oregon on certain days in April. Health officials said state test results looking for salmonella on food prep surfaces and food items came back negative. The investigation continues at a local level, but according to the environmental health program manager for DCPH, this salmonella outbreak is likely a case of cross contamination. Investigators have confirmed 30 people contracted salmonella after eating at the "Los Dos" from April 9 to April 17. Health officials have had not reported cases of people contracting salmonella outside of that date range. No deaths have been linked to the outbreak either. DCPH officials have been working with the restaurant for the last few weeks to make sure employees are following proper procedures, focusing on hand washing and food storage.
Source: http://www.kmtr.com/news/local/story/Cross-contamination-likely-in-Roseburg-Los-Dos/7DAtbT6QtEaRGN_k4ilrJA.cspx

27. *May 18, Alexandria Town Talk* – (Louisiana) **Norovirus may not be cause of Central deaths.** New test results may point to another cause for the deaths of three Central Louisiana State Hospital patients earlier this month. Initial test results led investigators with the Department of Health and Hospitals to believe the common norovirus is what led to more than 40 patients and staff at the Pineville facility getting sick and three patients dying May 7 and 8. But while some patients' stools tested positive for the virus, many did not. Now it is thought that norovirus isn't an "adequate explanation" for the illnesses and deaths, said the medical director for the Alexandria-based Region 6 of the DHH's Office of Public Health. Because of that doubt, a Centers for Disease Control team came to the Pineville behavioral health hospital to intensify the investigation. They stayed through May 17, working with local staff, collecting new samples, re-interviewing patients and staff, re-examining medical records and re-analyzing epidemiological data, the medical director said. He said new samples would be sent off to be tested for even more agents along with samples of all of the food in the kitchen that had been carefully saved and preserved, the medical director said. The medical director said all signs of sickness seem to have subsided, with the last instance of diarrhea occurring four days ago. "Clearly norovirus was there," he said. "The problem is there are a lot of causes of food poisoning. Some are bacterial, some are viral. And norovirus is nearly at the top of this list. But it does not seem to explain all of the cases and is not present enough to feel that it is 100 percent sure the cause of everything." He was unable to give specifics, but did say that not all of the patients who died tested positive for norovirus. The hospital's kitchen remains closed, and it won't reopen until all tests have come back. Once they are completed, the medical director said, the kitchen will undergo a "super cleaning." The hospital's staff has already begun to receive food-handling training.
Source: http://www.thetowntalk.com/article/20100518/NEWS01/5180322

28. *May 17, Standard-Examiner* – (Utah) **Nine sickened by campylobacter illness linked to raw milk.** An illness linked to raw milk has infected nine people in Utah. The Utah

Department of Health (UDOH) announced May 17 that two dairies in the state, including one in Weber County, had sold contaminated milk that made 15 people ill. Ropelato Dairy at 4019 W. 1800 South in Ogden was the source of the campylobacter outbreak that sickened nine people, according to spokespeople from the Utah Department of Agriculture and UDOH. Raw milk from a dairy in Richfield gave several people salmonella. Raw milk was approved for sale by the Utah Legislature in 2007 despite opposition from the U.S. Department of Agriculture (UDA) because of health concerns, a UDA spokesman said. "Raw milk, no matter how carefully handled, has risks," said a Weber-Morgan Health Department epidemiologist. Now raw milk, which is unpasteurized and goes from cow to refrigeration without treatment, is legally available for retail only through places permitted by the UDA. The milk is tested monthly for problems, and sales are suspended if bacteria is found, the UDA spokesman said. The milk is then tested weekly until it is within safety standards, when the raw milk can be sold again, he said. The co-owner of Ropelato Dairy, said they stopped selling raw milk after hearing of one person getting sick. He said they are not currently selling the milk and will decide whether to begin selling raw milk again. The Weber-Morgan Health Department epidemiologist said raw milk has made up about a third of the health department's campy cases in the last year.
Source: http://www.standard.net/topics/food/2010/05/17/nine-sickened-campylobacter-illness-linked-raw-milk

29. *May 17, Associated Press* – (Illinois) **Some farmers considering replanting flooded corn.** The Illinois Department of Agriculture said some farmers are considering replanting corn that has been sitting in water over the past week. The department said May 17 the amounts that may be replanted are small relative to the 12.6 million acres of corn Illinois farmers are expected to plant this year. Farmers got off to an early start this year and the state said 96 percent of the anticipated crop is in the ground. But wet, cool weather has been the rule the past week. A University of Illinois crop expert said that kind of weather leads to so-called lost days when the crop doesn't grow. He doesn't believe the weather, at least so far, is causing serious long-term problems.
Source: http://www.bnd.com/2010/05/17/1259538/some-farmers-considering-replanting.html

30. *May 16, USA Today* – (National) **USDA beefs up school meat-safety program.** Come fall, the ground beef used in school lunches will be as safe as ground beef sold to the nation's fast food chains — a major improvement, critics say. The U.S. Agriculture Department (USDA) announced May 14 that it will require all ground beef purchased for the National School Lunch Program to adhere to new safety standards after July 1. The program supplies ground beef, chicken and other food for more than 31 million schoolchildren. The rules bring school lunches "right in line with contemporary standards," said a food-safety consultant who developed a rigorous safety program for the Jack in the Box chain. "In fact, I'd make the case that the school lunch standards will now be above some of our major retail grocery chains." The USDA announced in February that it would raise standards for school lunches and has spelled those standards out in detail. The rules call for more stringent microbiological testing and said beef should be sampled every 15 minutes on production lines. Previously, ground

beef bound for schools was sampled an average of eight times during an entire production day, and then those samples were combined and subjected to testing once a shift. The rules make suppliers with "a long-term poor safety record" ineligible to sell to the school lunch program without a complete analysis of why their products failed inspections, said a spokesman for the USDA's Agricultural Marketing Service (AMS), which purchases beef for the school lunch program. No currently eligible contractors would be ineligible under that requirement "if it were in effect," he said.
Source: http://www.usatoday.com/news/education/2010-05-14-school-meat-safety_N.htm

For another story, see item **19**

[Return to top]

Water Sector

31. *May 18, Elgin Courier-News* – (Illinois) **Two face possible charges for dumping chemicals into Fox River.** Mavis Avenue neighbors were watching the carp, some as big as 12 pounds, meander in a stream that runs to the Fox River in South Elgin, Illinois Saturday evening when they noticed bubbling foam. Within minutes, the fish died and started floating to the surface. The Illinois Environmental Protection Agency placed a foam barrier across a creek that runs into the Fox River, just south of Mavis Avenue Monday. The creek had been polluted over the weekend, which resulted in dead fish and wildlife. Now, South Elgin police and state agencies, including the Illinois Department of Natural Resources and the Illinois Environmental Protection Agency, are investigating chemicals that were illegally dumped at a nearby Sundown Road business Saturday and affected the stream, authorities said. A man identified as the owner of Dy Recycling declined to comment Monday morning. No charges were filed as of late Monday against the two men police questioned Saturday evening after they were spotted pouring an unknown substance into the stormwater sewer system at that business. A cleanup crew, hired by that business owner, spent the morning dredging the stream and collecting the dead carp, catfish and water snakes. And South Elgin firefighters tentatively have identified two substances that were dumped as acid-based chemicals, the fire chief said. He did not release further details about the chemicals or how much was dumped. The substance had been poured into a storm drainage sewer, flowed into a retention basin on the property, then floated into a tributary of the Fox River. Neither drinking water supplies nor sanitary sewers were affected, according to the Fox River Water Reclamation District.
Source: http://www.suburbanchicagonews.com/couriernews/news/2282528,fox-river-chemical-dumping_EL051710.article

[Return to top]

Public Health and Healthcare Sector

32. *May 18, Bio Prep Watch* – (California) **Mumps outbreak may have entered Los Angeles County.** The Los Angeles Times reports that a mumps outbreak on the East Coast may have crossed the country to Los Angeles County. The newspaper reported May 16 that there have been nine cases of mumps reported in the county so far in 2010. That number is already two higher than what was reported in all of 2009. Of the nine cases reported so far, four may be related to a far larger outbreak in New York and New Jersey. There, the Times reports, more than 3,100 probable mumps cases have been reported, mostly in the Orthodox Jewish community. It is the largest outbreak in the U.S. in four years, according to the Los Angeles Times. The Los Angeles Times reports that the New York outbreak began in June 2009. An unvaccinated 11-year-old boy visited Britain, where mumps outbreaks are frequent. The paper states he then went to a summer camp and spread the disease.
Source: http://www.bioprepwatch.com/news/213073-mumps-outbreak-may-have-entered-los-angeles-county

33. *May 18, Orlando Sentinel* – (Florida) **Bomb threat partially evacuated St. Cloud hospital.** St. Cloud, Florida, police investigated a bomb threat that forced the partial evacuation of St. Cloud Hospital Monday morning. A male caller called the hospital about 6:18 a.m. to say that there was a bomb on the premises and then hung up. Officers went out to the hospital and a K-9 unit conducted a sweep of the facility and surrounding areas but did not find any evidence of an explosive device.
Source: http://www.orlandosentinel.com/news/local/breakingnews/os-bomb-threat-st-cloud-hospital-20100518,0,3206516.story

34. *May 17, ComputerWorld* – (National) **P2P networks a treasure trove of leaked health care data, study finds.** Nearly eight months after new rules were enacted requiring stronger protection of health care information, organizations are still leaking such data on file-sharing networks, a study by Dartmouth College's Tuck School of Business has found. In a research paper to be presented at an IEEE security symposium Tuesday, a Dartmouth College professor will describe how university researchers discovered thousands of documents containing sensitive patient information on popular peer-to-peer (P2P) networks. One of the more than 3,000 files discovered by the researchers was a spreadsheet containing insurance details, personally identifying information, physician names and diagnosis codes on more than 28,000 individuals. Another document contained similar data on more than 7,000 individuals. Many of the documents contained sensitive patient communications, treatment data, medical diagnoses and psychiatric evaluations. At least five files contained enough information to be classified as a major breach under current health-care breach notification rules. While some of the documents appear to have been leaked before the current administration's Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted, many appear to be fairly recent. A previous study by Dartmouth in 2008 also unearthed files containing health-care data floating on P2P networks, such as Limewire, eDonkey and BearShare. Among the documents found in that study was one containing 350 Megabytes of patient data for a group of anesthesiologists, and another with information on patients at an AIDS clinic in Chicago.

Source: http://www.computerworld.com/s/article/9176883/P2P_networks_a_treasure_trove_of_leaked_health_care_data_study_finds

35. *May 17, KJRH2 Tulsa* – (Oklahoma) **After meningitis outbreak, top state health officials weigh in.** In March, two students died and four others were hospitalized as a result of a meningitis outbreak in the Oolagah-Talala, Oklahoma, School District. It left lots of questions and concerns. Officials from the Oklahoma State Department of Health wanted to clear up confusion about proper mitigation and prevention. So they made a visit to the Tulsa County Health Department Monday for a round table discussion. Doctors said one of the best ways to prevent the disease is hand-washing. Source: http://www.kjrh.com/content/news/state/story/After-meningitis-outbreak-top-state-health/nSE1OiEDFUydpzxbT_w3DQ.cspx

36. *May 17, Vaccine News Daily* – (International) **Canada warns of second measles outbreak.** Five confirmed cases of measles in Alberta, Canada, have led to officials with Alberta Health Services requesting residents to get measles vaccines, according to iNews880.com. The five confirmed cases all occurred within the past week. Officials said the first confirmed case was a toddler a week ago. On May 14, Alberta Health Services officials reported there were four new confirmed cases. Even though the strain seems to be the same as a recent outbreak in British Columbia, the two outbreaks do not appear to be connected. More than two dozen people contracted the illness in British Columbia in April, according to assorted wire reports.
Source: http://vaccinenewsdaily.com/news/213068-canada-warns-of-second-measles-outbreak

[Return to top]

Government Facilities Sector

37. *May 18, The News-Press* – (Florida) **Suspicious cooler forces downtown Fort Myers road, building closures.** The Fort Myers police chief said the suspicious package found outside a federal building Tuesday, was in fact a cooler. He said the bomb squad was on the scene, but he didn't disclose what is inside the cooler. The Fort Myers police chief did not give an estimated time as to when the evacuation of downtown Fort Myers will be over. "We received a call from several concerned people," the police chief said. "There was a small cooler located by or near the federal courthouse. The concern from the federal marshal was there was something suspicious about it, so we went ahead and cordoned off the area." The police chief said several county departments are working at the scene and the bomb squad has also arrived. He said he believes the bomb squad may have already looked at the package. "I'm anticipating they will remove the package from this location and probably detonate it at another location," he said. The police chief would not elaborate on what could be in the cooler.
Source: http://www.news-press.com/article/20100518/NEWS0110/100518012/1075/Suspicious-cooler-forces-downtown-Fort-Myers-road-building-closures

38. *May 18, The Register* – (International) **NATO should tool up for cyber war, say globo-bigwigs.** The North Atlantic Treaty Organization (NATO) believes there is not likely to be a conventional military attack on its members in the future, but that some form of cyber-attack is one of three most probable dangers facing the alliance. The organization is the midst of finding itself a new purpose. A group of bigwigs have been appointed to find "a New Strategic Concept". NATO has gone through several changes since its creation in the wake of the Second World War as a defensive alliance against the Soviet Union. Although NATO said the possibility of conventional military attack could not be ignored, it is more likely to face an attack by ballistic missile, a terrorist attack or a cyber attack. Dealing with cyber attacks will require more cooperation with the European Union, the experts conclude, because the EU has more expertise in dealing with such attacks. The report warns: "The next significant attack on the Alliance may well come down a fiber optic cable. Already, cyber attacks against NATO systems occur frequently, but most often below the threshold of political concern." It recommends a major effort to increase monitoring of NATO's critical network in order to find and fix vulnerabilities. The Civil- Military Cooperation Centre for Excellence should improve members' training in cyber-defense. NATO members should expand their early-warning, network-monitoring systems. NATO should have a team ready to dispatch to areas under or threatened by cyber attack. Finally the experts said that over time, NATO should "plan to mount a fully adequate array of cyber-defense capabilities, including passive and active elements."
Source: http://www.theregister.co.uk/2010/05/18/nato_cyber_defence/

39. *May 18, WTVT 13 Tampa* – (Florida) **Security stepped up at Chamberlain High.** Students at Chamberlain High School in Tampa, Florida were greeted by extra security Tuesday morning, one day after a homemade acid bomb went off in a hallway and injured a student, putting the school on lockdown for several hours. Tampa police are providing additional security patrols Tuesday, saying they, along with school officials, are not taking the situation lightly. Authorities said they still have not determined who rolled the chemical-filled, plastic water bottle out of a classroom and into a hallway around 8:30 a.m. Monday. The device exploded, slightly burning an 18-year-old girl. A second acid bomb that did not detonate was found in a nearby bathroom while police were searching the school. Some students told FOX 13 Tuesday morning that they were somewhat hesitant coming to school. Monday, some students speculated that the incident may have been some sort of prank, but school officials said that doesn't matter and that they still plan to prosecute whoever is responsible.
Source: http://www.myfoxtampabay.com/dpp/news/local/hillsborough/security-stepped-up-at-chamberlain-high-051810

40. *May 17, IDG News Service* – (National) **Survey: Gov't agencies use unsafe methods to transfer files.** Employees at many U.S. government agencies are using unsecure methods, including personal e-mail accounts, to transfer large files, often in violation of agency policy, according to a survey. Fifty-two percent of the respondents to the survey of 200 federal IT and information security professionals said employees at their agencies used personal e-mail to transfer files within their agencies or to other agencies. About two-thirds of those responding to the survey said employees used

physical media, including USB drives and DVDs, to transfer files, and 60 percent of employees use FTP (File Transfer Protocol), according to the survey, completed by MeriTalk, a government IT social-networking site, and Axway, an IT security vendor. Forty percent of those surveyed said employees at their agencies use virtual private networks to transfer files and 34 percent said employees use Web-hosted, file-transfer services. Sending unencrypted data over FTP or personal e-mail, or putting it on physical media is a major problem for data security, the survey authors said. In March, the U.S. House of Representatives passed the Secure Federal File Sharing Act, which in many cases would prohibit government employees from using peer-to-peer file-sharing software, including FTP. The bill, sponsored by a Democratic congressman from New York, is awaiting action in the Senate.
Source:
http://www.computerworld.com/s/article/9176889/Survey_Gov_t_agencies_use_unsafe_methods_to_transfer_files

41. *May 17, Knoxville News Sentinel* – (Tennessee) **State agrees to extend cleanup at Molten Salt Reactor.** Environmental regulators are in dispute with the Department of Energy (DOE) on a number of issues regarding the Oak Ridge cleanup program, but the state of Tennessee has agreed - verbally at least - to give DOE more time to remove the highly radioactive fuel salts at the Molten Salt Reactor. Cleanup plans at the old reactor have been plagued with problems and delays, some due to the complex nature of the nuclear materials that have been housed there for decades.
Source: http://www.knoxnews.com/news/2010/may/17/state-agrees-extend-cleanup-molten-salt-reactor/

For more stories, see items **24** and **49**

[Return to top]

Emergency Services Sector

42. *May 18, Texarkana Gazette* – (Arkansas) **911 glitch forces city to rely on backup call center for nearly 2 hours, Monday.** A glitch in an electrical circuit at the Bi-State Central Communications Center meant Texarkana-area 911 calls were routed through a backup center for about an hour-and-a-half Monday night. The system failure happened about 8:30 p.m. “We’re not exactly sure what caused it but we had an electrical circuit in 911 that failed,” said the commander of Central Records and Communication division of the Texarkana, Arkansas, Police Department. “When this happened we immediately transferred calls to New Boston.”
Source: http://www.texarkanagazette.com/news/localnews/2010/05/18/911-glitch-forces-city-to-rely-on-backup-4.php

43. *May 17, WIVB 4 Buffalo* – (New York) **After copier fiasco, FTC may regulate.** It was a startling wake-up call for anyone using a digital copier. A CBS News investigation found confidential Buffalo, New York Police records in a copier sent to New Jersey. New federal regulations may follow. Four weeks after CBS News bought a few used

digital copiers and found sensitive Buffalo Police information still on them, a Massachusetts Congressman is calling for an investigation by the Federal Trade Commission. He said, "We have to do a lot more to ensure the public and corporations know this, and that absolute security is applied to copy machines across our country." The FTC has already responded, saying it shares the Representative's concern, and that it has begun reaching out to copier manufacturers and resellers to ensure that they are aware of the privacy risks and are warning customers of those risks. The city of Buffalo found out the hard way in January after trading in two old digital copiers from Buffalo Police Headquarters that ended up in a warehouse in New Jersey. CBS bought them for $300 apiece and on the hard drive were still lists of domestic violence complaints and targets of a major drug raid. On the same day, CBS bought an old copier that had been used by a health insurance company that still had confidential medical records on it.
Source: http://www.wivb.com/dpp/news/local/After-copier-fiasco-FTC-may-regulate

44. *May 17, Chicago Tribune* – (Illinois) **3 teens detained over stolen police guns.** On Monday, a Cook County, Illinois Juvenile Court judge ordered the detention of three youths after they were accused of stealing 25 guns from the Harvey, Illinois Police Department's shooting range. The three boys, who were handcuffed together, did not react when the judge agreed with prosecutors' request that the boys be kept in custody. Prosecutors cited an "urgent and immediate need" to keep them incarcerated.
Source: http://articles.chicagotribune.com/2010-05-17/news/ct-met-harvey-guns-hearing-20100517_1_shooting-range-three-boys-two-handguns

[Return to top]

Information Technology Sector

45. *May 18, Help Net Security* – (International) **Web browsers leave 'fingerprints' as you surf.** An overwhelming majority of Web browsers have unique signatures — creating identifiable "fingerprints" that could be used to track someone as they surf the Internet, according to research by the Electronic Frontier Foundation (EFF). The findings were the result of an experiment EFF conducted with volunteers who visited a Web site that anonymously logged the configuration and version information from each participant's operating system, browser, and browser plug-ins — information that Web sites routinely access each time one visits — and compared that information to a database of configurations collected from almost a million other visitors. EFF found that 84 percent of the configuration combinations were unique and identifiable, creating unique and identifiable browser "fingerprints." Browsers with Adobe Flash or Java plug-ins installed were 94 percent unique and trackable. EFF found that some browsers were less likely to contain unique configurations, including those that block JavaScript, and some browser plug-ins may be able to be configured to limit the information a browser shares with the Web sites one visits. But overall, it is very difficult to reconfigure a browser to make it less identifiable. The best solution for Web users may be to insist that new privacy protections be built into the browsers themselves.
Source: http://www.net-security.org/secworld.php?id=9303

46. *May 18, The Register* – (International) **Koobface gang counter-poohpooh nemesis sec-pro Danchev.** The gang behind the infamous Koobface worm has responded to a post by a security researcher on their activities and motives with an answer buried in the latest version of their malware. A noted security researcher posted a list of "10 things you didn't know about the Koobface gang" in a blog post back in February. Koobface (an anagram of Facebook) is a worm that spreads on social networking sites. The worm, reckoned to be one of the most complex strains of malware yet seen, steals information from compromised hosts and promotes scareware sites, according to the researcher and anti-virus firms. Or not, according to the VXers behind the code. Late last week "Ali Baba" of the Koobface gang posted a point by point response as a message on Koobface-infected hosts, which served scareware disguised as bogus video codecs. Essentially the gang members attempt to paint themselves as elite coders in it for the lolz and not the loot. "What makes an impression is their attempts to distance themselves from major campaigns affecting high-profile U.S. based Web properties, fraudulent activities such as click fraud, and their attempt to legitimize their malicious activities by emphasizing the fact that they are not involved in crimeware campaigns, and have never stolen any credit card details," the researcher explained.
Source: http://www.theregister.co.uk/2010/05/18/koobface_top_10_facts/

47. *May 18, ComputerWorld* – (International) **Huge 'sexiest video ever' attack hits Facebook.** A huge attack by a rogue Facebook application last weekend infected users' PCs with popup-spewing adware, a security researcher said May 17. On May 15, AVG Technologies received more than 300,000 reports of the malicious Facebook app, said AVG's chief research officer. AVG came up with its tally by counting the number of reports from its LinkScanner software, a free browser add-on that detects potentially poisoned pages. "It was stunning, really, the number," said the research officer in an interview via instant message late May 17. "And stunning that it was not viral or wormy [but that] Facebook did it all by itself." The volume of reports on the May 15 rogue Facebook software was highest during the nine-hour period between midnight and 9 a.m. Eastern Standard Time, with spikes of approximately 40,000 per hour coming at 7 a.m. and noon. For the day, AVG received more than 300,000 reports, triple that of AVG's second-most-reported piece of spyware. According to the researcher, Facebook eradicated the rogue application about 15 hours after the attack started. Facebook's only acknowledgment of the attack came on its security page, where a "Tip of the Week" early May 17 read: "Don't click on suspicious-looking links, even if they've been sent or posted by friends." But other security firms also noted the attack. Both U.K.-based Sophos and U.S. security company Websense dubbed the attack "Sexiest video ever," based on the message that appeared on Facebook users' walls, seemingly from their Facebook friends.
Source:
http://www.computerworld.com/s/article/9176905/Huge_sexiest_video_ever_attack_hits_Facebook

48. *May 18, PC Advisor UK* – (International) **USB worm named biggest PC threat.** A worm that is spreading via USB flash drives has been named the biggest security threat to PC users by McAfee. According to the security vendor's Threats Report: First

Quarter 2010, an AutoRun-related infection was also the world's third biggest PC threat during the first three months of the year, while the rest of the top five biggest PC threats were made up of password-stealing Trojans. The report revealed that spam rates have remained steady. However, there has been an increase in diploma spam, or spam that offers forged qualifications, in China, South Korea and Vietnam. McAfee also said malware and spam in Thailand, Romania, the Philippines, India, Indonesia, Colombia, Chile, and Brazil had surged. The security vendor said this was due to the significant growth of Web use in these countries coupled with a lack of security awareness. "Our latest threat report verifies that trends in malware and spam continue to grow at our predicted rates," said a senior vice president and chief technology officer of Global Threat Intelligence for McAfee. "Previously emerging trends, such as AutoRun malware, are now at the forefront."
Source: http://www.networkworld.com/news/2010/051810-usb-worm-named-biggest-pc.html?hpg1=bn

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

49. *May 18, GPS Daily* – (National) **Delta IV GPS IIF-01 launch set May 20.** The U.S. Air Force will launch the first Global Positioning System Block IIF satellite aboard a United Launch Alliance Delta IV Evolved Expendable Launch Vehicle from Space Launch Complex 37 in Cape Canaveral, Florida May 20. The GPS IIF system brings next-generation performance to the constellation. The GPS IIF vehicle is critical to U.S. national security and sustaining GPS constellation availability for global civil, commercial and defense applications. Besides sustaining the GPS constellation, IIF features increased capability and improved mission performance and longevity. Not only is it the first IIF to be launched, this will be the first GPS satellite to ride on the Delta IV launch vehicle.
Source: http://www.gpsdaily.com/reports/Delta_IV_GPS_IIF_01_Launch_Set_May_20_999.html

50. *May 17, DarkReading* – (International) **Five ways to (physically) hack a data center.** A company can spend millions of dollars on network security, but it is all for naught if the data center has physical weaknesses that leave it open to intruders. Red team experts hired to social engineer their way into an organization said they regularly find physical hacking far too easy. A senior security consultant with Trustwave's SpiderLabs, said data centers he has investigated for security weaknesses commonly

have the same cracks in the physical infrastructure that can be exploited for infiltrating these sensitive areas. The five simplest ways to hack into a data center are by crawling through void spaces in the data-center walls, lock-picking the door, "tailgating" into the building, posing as contractors or service repairman, and jimmying open improperly installed doors or windows.
Source:
http://www.darkreading.com/database_security/security/management/showArticle.jhtml?articleID=224900081

51. *May 17, IDG News Service* – (National) **FTC asked to investigate Google Wi-Fi 'snooping'.** A consumer group has called on the U.S. Federal Trade Commission (FTC) to investigate Google after the search company revealed that it had been collecting people's Internet communications from open wireless networks. On May 14, Google said it would stop its Street View cars from sniffing wireless networks after discovering that they had been collecting unencrypted content — the contents of Web pages, for example — unbeknownst to Google. Consumer Watchdog said the FTC should find out exactly what Google logged, how long it collected the information and what it ended up doing with it. "Google has demonstrated a history of pushing the envelope and then apologizing when its overreach is discovered," the group said Monday in a press release. "Given its recent record of privacy abuses, there is absolutely no reason to trust anything the Internet giant claims about its data collection policies." Google was collecting the Wi-Fi data — SSID (Service Set Identifier) information and MAC (Media Access Control) addresses — in order to get better location information for its Google Maps service.
Source:
http://www.computerworld.com/s/article/9176902/FTC_asked_to_investigate_Google_Wi_Fi_snooping_

[Return to top]

Commercial Facilities Sector

52. *May 18, Republican-American* – (Connecticut) **Fire rips through Naugatuck shopping plaza; cause not determined.** Three businesses are temporarily shut down after fire ripped through a shopping plaza on Quinn Street in Naugatuck, Connecticut late May 16. Fire broke out in a basement at the plaza, which houses five businesses tucked in the middle of a residential neighborhood at 147-153 Quinn St. Nobody was in any of the stores, and therefore nobody was injured. Firefighters are trying to figure out what caused the blaze, which began in a storage facility underneath the hair salon. Three storefronts sustained significant damage. The other businesses sustained smoke damage that was expected to be cleaned soon. Another storefront is vacant. The building also had damage to electrical wires and gas lines in the basement, above where the fire started. The storage room where the fire began was filled with furniture, automotive parts, oil, grease, acetylene and propane. Firefighters were busy May 17 trying to clean out the storage facility to pinpoint the fire's origin.
Source: http://www.rep-am.com/news/local/483843.txt

53. *May 18, The Mercury News* – (Pennsylvania) **Honey Brook establishment evacuated after bomb threat.** Thirty-three people were evacuated from the Maple Inn Sunday night in Honey Brook, Pennsylvania after a bomb threat was called in to the 3125 Horseshoe Pike establishment. According to police, a pool tournament was going on at the restaurant when a staff member answered the phone about 4:25 p.m. and was told by the caller that there was a bomb in the inn. The caller, who did not identify himself to the staff member, then hung up. The staff of the inn immediately notified state police in Embreeville who advised them to evacuate the inn of its 30 patrons and three staff members. State police, with the assistance of the Honey Brook Fire Department, closed Route 322 in both directions from Cambridge Road to Birdell Road and moved nearby residents to a safe location before the state police bomb squad searched the inn with the help of a K-9 officer. No explosive devices were found inside the Maple Inn. Route 322 was closed for three hours while the search was conducted.
Source:
http://www.pottstownmercury.com/articles/2010/05/18/blotter/doc4bf2832e3e03b570342038.txt

54. *May 17, Reed Construction Data* – (National) **New rule for contractors to prevent lead contamination.** As of April 22, 2010, contractors must be certified and follow specific work practices to prevent lead contamination when performing renovation, repair and painting projects in housing and child-occupied facilities built before 1978. The new U.S. Environmental Protection Agency (EPA) rule is aimed at preventing lead poisoning in children and adults and applies to renovation, repair and painting projects that disturb more than six square feet of potentially contaminated lead-based painted surfaces. What the rule will certainly do is directly affect the wallets of contractors, homeowners, property managers and municipalities alike. To comply with the rule, renovation contractors, painters, maintenance workers in multi-family housing, and workers in other specialty trades can expect to incur direct costs of $315 for a one-day certification course. The certification course trains workers on how to contain the work area, minimize dust and perform thorough clean up. Additional contractor costs include $300 for the EPA certification, as well as costs for any new equipment, such as respirator cartridges and HEPA vacuum filters. Non-compliance can be significantly more expensive at $37,500 per day per violation. For homeowners, schools, childcare facilities and others, the additional time and labor associated with lead-contamination prevention will increase the cost to repair, renovate or remodel. This could lead some to hire uncertified contractors or avoid needed repairs altogether.
Source: http://www.reedconstructiondata.com/news/2010/05/new-rule-for-contractors-to-prevent-lead-contamination/

55. *May 16, WTMJ 4 Milwaukee* – (Wisconsin) **Time-share building evacuated at Grand Geneva.** Several people were evacuated from the Holiday Inn Club Vacations at the Grand Geneva Resort in Lake Geneva, Wisconsin after a “chemical odor” was reported the night of May 14. According to the Walworth County Sheriff’s Office, cleaning chemicals were combined in a maintenance room causing the odor. The time-share building was evacuated for an hour and a half for cleaning and ventilation. Some 25 families were moved to other buildings at the resort. An employee was overcome by

the odor and was transported to a local hospital.
Source: http://www.todaystmj4.com/news/local/93872364.html

For another story, see item **16**

[Return to top]

National Monuments and Icons Sector

56. *May 18, KTVK 3 Phoenix* – (Arizona) **Crews battling Fraguita wildfire in Coronado National Forest.** Crews are dealing with another major wildfire that is growing near in southern Arizona near the border. Firefighters have named the fire the Fraguita fire. So far nearly 1,000 acres have been burned. The fire is burning just south of Arivaca in the Coronado National Forest. Nearly 100 firefighters are working to contain the Fraguita fire. An 80 percent perimeter has been set to contain the blaze. Strong winds are expected in this part of the state Tuesday, which could make it even more difficult to fight the wildfire.
Source: http://www.azfamily.com/news/Crews-battling-Fraguita-wildfire-in-Coronado-National-Forest-94115799.html

[Return to top]

Dams Sector

57. *May 17, WSOC 9 Charlotte* – (North Carolina) **Neighbors worried about possible dam breach.** A dam in Lowell, North Carolina, that broke apart is holding together after some repairs, but neighbors are worried that the event could happen again. Overnight crews put a second pump in to manage the rainwater that poured over the dam this weekend. “This is a temporary dam the county installed while they work to complete a bigger dam. It will turn this into a lake for nearby Poston Park,” one resident said. Another resident said the dam has done nothing but widen what once was a small creek in their backyard and created rapids when it rains. The emergency management director visited the dam Monday morning after water poured over the dam Sunday. “The temporary dam has not been damaged. The integrity is still there,” he said. He said the construction was approved by the state but he added there is no predicting the weather. More unexpected storms can cause problems here. Work crews said they will make sure the work does not threaten the people in the five homes along the creek. The crews are about to install a pipe that will allow them to manage the water flowing into this area.
Source: http://www.wsoctv.com/news/23583277/detail.html

58. *May 17, WPXI 11 Pittsburgh* – (Pennsylvania) **Corps urges major work on Pittsburgh locks, dams.** Federal officials are again urging major work on the locks and dams on Pittsburgh’s three rivers. The Army Corps of Engineers hosted a tour Friday of the Emsworth locks to highlight preliminary study recommendations calling for complete replacement of the chronically failing locks that channel boats around three

dams on the Ohio River northwest of Pittsburgh. Millions of tons of coal, chemicals, metals, and other cargo are shipped annually on the water highway of the Monongahela, Allegheny and Ohio rivers. The locks are essentially water-driven elevators that lift and lower boats so they can pass through dams, which control water levels on the river enabling navigation. With Emsworth partly out of service for repairs, it was taking towboats 15 or 16 hours to get their coal barges through, a process that normally takes about two hours. The Corps chief of locks and dams said a typical tow costs $500 per hour to operate. “If you’re sitting there 10 hours, $5,000 just went down the tubes,” he said. And such costs trickle down to consumers. The Emsworth Locks and Dams were completed in 1922, and the next two facilities downstream are not much younger. An Upper Ohio Navigation Study is to be completed in November 2011, but financing and construction of new facilities could take another 20 years or more. And the cost is estimated at $2 billion, with another $1 billion to fix similar problems on the Monongahela River’s locks and dams. With the main 600-foot-long and 110-foot-wide lock chamber at Emsworth drained, it was possible Friday to descend to the dried-out river floor, where crews were working to repair the archaic valve system that allows the lock operator to drain water from the chamber. Large cracks, gaps and pockmarks were visible on the concrete walls, and officials said they fear a possible collapse.
Source: http://www.wpxi.com/news/23579325/detail.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact Information

Content and Suggestions:	Send mail to 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