Homeland Security

Daily Open Source Infrastructure Report for 20 May 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- The Boston Globe reports that the Boston Fire Department (BFD) said a chlorine leak in a truck near Boston College has been contained. A BFD spokesman said an entry team of firefighters found one of the chlorine cylinders was leaking on the box truck Tuesday. "They fixed the leak and ventilated the vehicle," he said. People were being allowed back on the college's campus, where two buildings had been evacuated, and Beacon Street is being reopened in the area. (See item **6**)
- According to The McDowell News, a mixture of chemicals at Walmart in McDowell County, North Carolina Tuesday evening, forced the evacuation of the store and sent a dozen people to the hospital. The Marion, North Carolina fire chief said an employee combined a couple of cleaners in the back of the store in preparation of scouring the bathrooms. (See item **70**)

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 18, Associated Press* – (Oregon) **Ore. needs time to evaluate power plant shutdown.** Oregon regulators need more time to evaluate Portland General Electric's plan for an early shutdown of Oregon's only coal-fired power plant. The Oregon Department of Environmental Quality said Tuesday that the agency supports closing the Boardman power plant early, but needs more time to evaluate how much pollution will be allowed during the last years of its life. So they will recommend the Environmental Quality Commission not approve the early shutdown at its June 17 meeting. PGE's Boardman plant is a major source of greenhouses gases and smog. The utility has offered to shut it down in 2020 - 20 years ahead of schedule - if it does not have to spend more than $400 million on new pollution controls.
   Source: http://www.forbes.com/feeds/ap/2010/05/18/business-multiutilities-financial-impact-us-pge-coal-plant-oregon_7616611.html?boxes=Homepagebusinessnews

2. *May 18, U.S. Department of Justice* – (Ohio) **Ohio utility to settle Clean Air Act violations.** American Municipal Power (AMP), an Ohio non-profit utility, will permanently retire its Richard H. Gorsuch Station coal-fired power plant near Marietta under a settlement to resolve violations of the Clean Air Act, the Justice Department and U.S. Environmental Protection Agency (EPA) announced May 18. As part of the settlement, AMP will also spend $15 million on an environmental mitigation project and pay a civil penalty of $850,000. "This settlement will remove harmful emissions from this coal-fired power plant by tens of thousands of tons each year and will significantly benefit air quality," said an Assistant Attorney General for the Justice Department's Environment and Natural Resources Division. The Gorsuch Station has a sulfur dioxide emission rate in the highest three percent of coal-fired utility sources in the country. AMP will permanently retire the Gorsuch Station by December 31, 2012, and implement interim sulfur dioxide and nitrogen oxide emission limits until that date. The settlement requires AMP to spend $15 million on energy efficiency services in lighting, refrigerator replacement and removal, and installation of building heating and cooling systems to all of the municipalities and their customers served by the Gorsuch Station. The energy efficiency services are designed to achieve a minimum reduction of 70,000 megawatt hours.
   Source: http://www.justice.gov/opa/pr/2010/May/10-enrd-585.html

For another story, see item 77

[Return to top]

Chemical Industry Sector

3. *May 19, Associated Press* – (International) **Cameroon: Pirates seize 2 Russian sailors.** Pirates kidnapped two Russian sailors during an attack on a cargo ship off the coast of Cameroon, the latest act of violence along West Africa's increasingly insecure coast, a private security official said Wednesday. The official told The Associated Press about 20 armed pirates boarded the MV North Spirit, a cargo ship carrying fertilizer and soya beans, as it docked Sunday night off Cameroon's commercial capital of Douala. The official said the pirates forced the sailors to lay face down on the upper

deck as they stole the ship's equipment and the sailors' personal belongings. The pirates then took the ship's captain and chief engineer hostage, the official said, adding that there has been no ransom demand.
Source: http://www.google.com/hostednews/ap/article/ALeqM5jrkyjzze25-J18rMG5Q-MqFAa9qAD9FPTVHG2

4. *May 19, Deseret News* – (Utah) **Tanker tips on I-215.** Southbound and northbound lanes of I-215 were closed after a tanker trailer rolled Tuesday afternoon in Salt Lake City, Utah. Around 3 p.m., emergency crews, including hazardous materials personnel, responded to the wreck at about 2700 North, according to a police officer. A semitrailer was apparently towing three tanker trailers when the last trailer broke away from the truck. The trailer rolled and dumped its contents. Radio traffic indicated the spill involved 24,000 gallons of magnesium chloride, which an emergency responder said would not have an environmental impact. Magnesium chloride is a form of liquid salt which has uses that include deicing roads. All lanes were temporarily closed from Redwood Road to 2200 North while crews determined what the spilled substance was. No other vehicles were involved in the accident.
Source:
http://www.fireengineering.com/index/articles/Wire_News_Display/1188842586.html

5. *May 19, KATC 3 Lafayette* – (Louisiana) **1-10 E between Rayne and Duson re-opened.** More than 18 hours after it was closed, I-10 E between the towns of Rayne and Duson has re-opened, Louisiana State Police tell KATC. The highway was closed Tuesday morning when an 18 wheeler turned on its side near mile marker 90, spilling a chemical called ethyleneamine that haz-mat teams had to come and clean up.
Source: http://www.katc.com/news/i-10-e-between-rayne-and-duson-re-opened/

6. *May 18, Boston Globe* – (Massachusetts) **Chlorine leak near BC is fixed.** A chlorine leak in a truck near Boston College has been contained, the Boston Fire Department said. A spokesman said an entry team of firefighters found one of the chlorine cylinders was leaking on the box truck Tuesday. "They fixed the leak and ventilated the vehicle," he said. People were being allowed back on the college's campus, where two buildings had been evacuated, and Beacon Street is being reopened in the area. The truck for Airgas, a company that distributes industrial and medical gases, had delivered 10 chlorine tanks to the Dedham Water Department, and was on its way to deliver gases to the college when the driver noticed there might be residual chlorine leaking from an empty cylinder, authorities said. "The driver noticed a possible leak, pulled over about 12:15 p.m., and notified the fire department," the spokesman said. Officials declared a Level 3 Haz-mat situation, shutting down a section of Beacon Street from the Chestnut Hill Reservoir to College Road in Newton, Massachusetts. No injuries were reported. A Boston College spokesman said the Merkert Chemistry Building and Campion Hall, which houses the Lynch School of Education, had been evacuated. He said that classes at the college were already over and today was the last day of exams so there were few students around. The truck had picked up eight empty chlorine cylinders at the Dedham Water Department. It was also carrying propane and hydrogen gas in separate tanks inside the vehicle.

Source:
http://www.boston.com/news/local/breaking_news/2010/05/chlorine_spills.html

7. *May 18, WTSP 10 St. Petersburg* – (Florida) **Stauffer Chemical Company site cleanup begins.** After more than f15 years of planning, the cleanup has begun on the site of the Stauffer Chemical Company along Anclote Road in Tarpon Springs, Florida. The facility produced elemental phosphorus between 1947 and 1981, switching hands between the Victor Chemical Company and Stauffer Chemical Company in the 1960's. When the site was permanently dismantled in 1983, a toxic wasteland was left behind. The EPA lists the most concerning soil contaminants as arsenic, antimony, beryllium, radium, elemental phosphorus, and polynuclear aromatic hydrocarbons. The EPA said it is possible workers at the plant were exposed to chemicals including asbestos and lead. A study of 36 former workers by the Agency for Toxic Substances and Disease Registry (ATSDR) found that 70 percent of the workers had mild to moderate respiratory problems. However, the cause could not be blamed on the plant alone. Other factors such as previous illness and smoking may also be aggravators, a rep. said. An ATSDR report calls on OSHA to follow up with former workers, and advises current workers on the site to wear protective gear while working around the contaminated soil. Regular air monitoring is also recommended to make sure people who live and work around the property are not exposed to the contaminants. The EPA said the air is being monitored every 15 minutes around the site. Stauffer is picking up the clean-up tab of $20 million. The project is expected to wrap up next summer. Source: http://www.wtsp.com/news/local/story.aspx?storyid=132331&catid=8

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *May 19, Brattleboro Reformer* – (Vermont) **VY reports mishap in cooling system test.** A test of Vermont Yankee's emergency core-cooling system Sunday resulted in "an unanticipated action," wrote a spokesman in an e-mail to the media. The Nuclear Regulatory Commission requires a test of the nuclear power plant's integrated emergency core-cooling system every 18 months, a spokesman told the Reformer May 18. The test simulates a loss of coolant accident and is done to ensure that the systems that deliver cooling water to the reactor are operating correctly, he said. For a reason that has not yet been determined, the water level in the reactor vessel was set higher than normal, the spokesman wrote. "When the test began and steam valves automatically realigned, some of the excess water (above the steam lines) drained through a steam line to the torus which contains a backup supply of cooling water and is located in the reactor building," he wrote, adding there were no safety consequences. A nuclear safety advocate involved in reviewing the plant's reliability, said it appears technicians added too much water to the reactor during the test. "Water overflowed into the steam lines which normally contain only steam," he said. "The steam lines need to be dry, as water can damage the turbine. "No damage was done even though water went down the steam line," the spokesman told the Reformer. Even though the event "was not immediately reportable," wrote the spokesman, "plant management has taken

steps to ensure this is not repeated in future tests."
Source: http://www.reformer.com/localnews/ci_15114447

9. *May 19, Reuters* – (Maryland) **Constellation Md. Calvert 1 reactor to exit outage.** Constellation Energy Nuclear Group's 873-megawatt Unit 1 at the Calvert Cliffs nuclear power plant in Lusby, Maryland started to exit an outage and ramped up to 15 percent power by early Wednesday, the Nuclear Regulatory Commission said in a report. The unit shut May 12 after losing its ability to transmit power to the grid.
Source: http://www.reuters.com/article/idUSN1921516020100519?type=marketsNews

10. *May 19, Associated Press* – (New York) **Indian Point likely to survive state ruling.** Concerns for Hudson River fish and other creatures have raised the prospect that the biggest power producer in the New York metropolitan area could be shut down. But closing the Indian Point nuclear plant in Buchanan would slash as much as 38 percent of the energy available to a power-hungry region and deprive plant owner Entergy Nuclear of hundreds of millions of dollars in profits. That leads many experts to believe there are real-world solutions well short of a shutdown. A New York agency refused last month to grant a water-quality permit needed for federal relicensing to keep the Indian Point plant operating into the 2030s. At issue is how Indian Point uses the river water. Thousands of fish and fish eggs are now sucked into the plant and killed or injured, including the shortnose sturgeon, which is an endangered species in New York.
Source: http://www.recordonline.com/apps/pbcs.dll/article?AID=/20100519/NEWS90/100519637

11. *May 18, Augusta Chronicle* – (Georgia) **Plant Vogtle drill set for today.** Would area residents know what to do if a serious nuclear accident occurred at Plant Vogtle in Waynesboro, Georgia? A major exercise May 18 will be monitored by the Federal Emergency Management Agency and the U.S. Nuclear Regulatory Commission (NRC) as a host of state and local agencies test Southern Nuclear's network of warning sirens, radio signals and emergency-response activities. "This will be one of the full-scale emergency exercises," a NRC spokesman said. He said it would start this morning and run through early afternoon. The event will focus on the procedures for notifying the public of an accident — and any needed responses or evacuations involving residents living within a 10-mile radius of the Burke County plant. Although emergency drills are conducted several times each year at nuclear power plants, larger exercises such as the one planned this week usually occur every other year, the NRC spokesman said. "It gives plant staff and support personnel a chance to do something they don't do on a day-to day-basis," he said. "But one thing they don't do is actually evacuate any people because that could end up putting people more at risk."
Source: http://chronicle.augusta.com/latest-news/2010-05-18/plant-vogtle-drill-set-today?v=1274223427

[Return to top]

Critical Manufacturing Sector

12. *May 19, Associated Press* – (National) **Toyota pays $16.4M fine for slowness in pedal case.** Toyota Motor Corp. paid a record $16.4-million fine yesterday for a slow response in its accelerator pedal recall. A Transportation Department official said the Japanese automaker paid the fine after reaching an agreement with the government April 19. Toyota had 30 days to pay it. The official was not authorized to speak publicly before an announcement was made. Toyota faced the maximum penalty allowed under law after it was accused of hiding earlier defects involving gas pedals. Toyota rejected the accusation even though it agreed to pay the fine. The world's largest car manufacturer has recalled more than 8 million vehicles worldwide for safety defects that affect some of its best-selling models. The company still faces hundreds of state and federal lawsuits in the United States. The Transportation Department is reviewing thousands of Toyota documents and could issue penalties over the company's handling of other safety recalls. Toyota confirmed paying the fine but declined further comment.
Source: http://toledoblade.com/article/20100519/BUSINESS02/5190335/-1/BUSINESS

13. *May 19, Associated Press* – (National) **FBI says box at San Antonio plant from inventor.** The FBI said an inventor from Nigeria apparently pitching a product is responsible for a suspicious package that led a police bomb squad to a Toyota manufacturing plant in San Antonio. An FBI Special Agent told WOAI Radio that the package was from an inventor with an idea for a turn signal. The inventor mailed the device to Toyota plants across America. The package with electronic parts reached the San Antonio plant Monday. The agent said Tuesday night that the FBI determined the device appeared to be a prototype. A Toyota spokeswoman said packages also sent to Kentucky and West Virginia were found to be non-threatening. A similar package led to the evacuation of an Indiana post office. Toyota did not immediately say whether it would consider the inventor's device.
Source: http://www.statesman.com/news/texas/fbi-says-box-at-san-antonio-plant-from-696629.html

14. *May 18, Tarentum Valley News Dispatch* – (Pennsylvania) **Ludlum to pay $1.6M pollution penalty.** Allegheny Ludlum Corporation has reached a settlement with federal and county agencies regarding alleged violations of the Clean Air Act at its Natrona, Pennsylvania melt shop. The agreement announced Monday by the federal Environmental Protection Agency (EPA) and U.S. Department of Justice calls for Ludlum, a subsidiary of Allegheny Technologies Inc. (ATI) which makes speciality stainless steel, to pay a $1.6 million civil penalty. That penalty will be divided equally between the federal government and the Allegheny County Health Department. In addition, Allegheny Ludlum agreed to permanently cease steel-making operations at it Natrona facility no later than November 30, 2010. The Natrona melt shop works in conjunction with the nearby Brackenridge Works where finished stainless steel is produced. It is scheduled to close as part of a physical restructuring of the plant, which includes a consolidation of the Natrona and Brackenridge melt shops. That will be followed by construction of a state-of-the-art hot strip mill expected to cost $1.5 billion. "This settlement will bring cleaner air to Allegheny County," said the EPA Mid-

Atlantic administrator. “We’re pleased that we could resolve these issues without further litigation, meaning nearby communities will benefit sooner from improved air quality,” he added. “We think this is as good an outcome as anybody could expect;” said a spokesman for ATI. The violations were discovered during an Aug. 8, 2007 EPA inspection of the Natrona facility. Emissions made up of volatile and semi-volatile organic compounds, nitrogen oxides, carbon monoxide, soot, including particulates greater than 10 microns and other hazardous air pollutants were seen escaping from the plant.
Source: http://www.pittsburghlive.com/x/valleynewsdispatch/s_681695.html

15. *May 18, WFRV 5 Green Bay* – (Wisconsin) **Report released on fire, explosion that killed firefighter.** An investigation has been completed into the 2009 dumpster fire at Bremer Manufacturing in New Holstein, Wisconsin that killed a St. Anna, Wisconsin firefighter. On December 29, 2009 a dumpster caught fire at Bremer Manufacturing. Calumet County Sheriff Deputies and the St. Anna Fire Department were dispatched to the scene. While attempting to subdue the flames with water and suppressant foam, an explosion occurred from within the dumpster; killing one volunteer firefighter and injuring eight others. The incident has been thoroughly investigated by the Department of Justice Fire Marshal’s Office, Calumet County Sheriff’s Department, and the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives, and was found to be of undetermined cause. Based on all available information, the investigative team made several determinations. The fire originated within the damaged refuse container, which contained aluminum alloy shavings and 55-gallon steel barrels of aluminum dross (slag). The cause of the fire is classified as “undetermined,” however there is no information available to indicate that the fire was as the result of an intentional act. The cause of the explosion was a result of thefire-suppression efforts and the introduction of water and fire-suppressant foam.
Source: http://www.wfrv.com/news/local/94182139.html

16. *May 18, Visor Down Motorcycle News* – (National) **BMW brake recall: the official word.** BMW Motorrad has announced the recall of R-Series boxer-twin and K 1200 GT motorcycles, manufactured between August 2006 and May 2009, after a potential fault in a brake pipe was diagnosed. It is possible that vibrations on affected motorcycles could cause the front brake pipe to leak and, over an extended period of time, cause brake fluid to escape. BMW Motorrad sought to reassure customers that the number of motorcycles, in which leaking brake pipes was noticed, is very small (one-tenth of a percent). No accidents have arisen as a result of this fault. In the event of a problem, riders will notice the leaking brake fluid or a reduction in the brake fluid level in the handlebar mounted brake fluid reservoir. This may result in a gradual loss of braking performance of the front brake. The rear brake is not affected. The BMW Motorrad dealer network plans to contact all customers who own motorcycles potentially affected by this fault.
Source: http://www.visordown.com/motorcycle-news--general-news/bmw-brake-recall-the-official-word/11495.html

[Return to top]

Defense Industrial Base Sector

17. *May 19, WTOP 1500 Washington* – (International) **Pilot error likely in combat crash.** Pilot error is likely to blame for the first crash of a CV-22 Osprey in a combat zone, the press has learned. Air Force investigators said the Osprey in Afghanistan was simply flying too low and hit an embankment, a source briefed on the finding said. The CV-22, which can tilt its rotors to fly like a plane, was in airplane mode when its blades struck an earthen berm, shearing off the wings and flipping it over. The conclusions rule out mechanical malfunction and hostile fire as possible causes, but they haven't been finalized yet. But an aviation writer and author of "The Dream Machine," said people should not rush to blame the dead pilot: "Whether a pilot is actually negligent or not is a very difficult question," he said. "I don't think it means anything for the future of the V-22, because obviously that kind of thing could happen to any aircraft." When the special operations Osprey went down last month, four on board died. Another 16 people survived.
Source: http://wtop.com/?nid=25&sid=1960593

18. *May 18, Military Times* – (Virginia) **Northrop: Ford's design issues minimal.** Engineers building the new aircraft carrier Gerald R. Ford (CVN 78) are making some design changes to avoid "electrical cable routing issues" that could interfere with some internal arrangements. The problems have been found "in limited areas of the ship design," said a spokesperson for Northrop Grumman Shipbuilding. "As can happen with any lead ship of the class performing first-of-a-kind activities, we have identified some interferences between cable arrangements and other design features that require correction. In these cases, changes to the design are being made and lessons learned applied," the spokeswoman said. Those changes include moving some wireways where electrical cable is strung and changing some cable supports, she added. "These issues are not widespread. We have not yet run any cable, but a small percentage of the cable supports that have been installed may require alteration." The impact on the ship's cost or construction schedule is still being evaluated, she said, "but expect it to be minimal." The Navy's Sea Systems Command (NAVSEA) acknowledged the problem but downplayed the impact. "The Navy is aware that [Northrop Grumman Shipbuilding] has identified some interferences between cable arrangements that require correction," NAVSEA said in an e-mail statement May 14. "The Navy understands this to be a small percentage of the cable arrangement design to date and results in no module fit-up issues." The ship, first of a new class of carriers, is under construction at Northrop's shipyard in Newport News, Va. More than 61 percent of the structural modules for the Ford are already complete, the spokeswoman said. "The fit-up of CVN 78 structural modules is as good or better than previous Nimitz-class carriers," she added.
Source:
http://www.militarytimes.com/news/2010/05/navy_defense_ford_electrical_051810w/

19. *May 18, Global Security Newswire* – (Tennessee) **Y-12 plant receives ovens for nuke parts testing.** The Y-12 Nuclear Security Complex in Tennessee has begun placing convection ovens at its primary assembly and dismantlement site for testing the ability

of nuclear-weapon parts to withstand the effects of time and environmental degradation, the Knoxville News Sentinel reported May 17. Officials at the National Nuclear Security Administration's Y-12 site office refused to specify whether the $22.6-million project would be used for testing highly enriched uranium. "What we use these ovens for is part of what we call the surveillance and certification program," the Y-12 site manager said, adding that the "thermal cycle" would expedite the testing process. "You are putting the components through environments that you want to, then evaluate the effects of those environments on those components," he said. The new plant, replacing work previously done in a section of another facility, is expected to begin operations in spring 2012.
Source: http://www.globalsecuritynewswire.org/gsn/nw_20100518_4787.php

20. *May 17, United States Department of Justice* – (National) **Two Chinese nationals convicted of illegally exporting electronics components used in military radar & electronic warfare.** Following a five-week trial, a federal jury in Massachusetts found two Chinese nationals, one of whom resided in the United States, guilty of illegally conspiring to violate U.S. export laws, and illegally exporting electronic equipment from the United States to China, the Justice Department announced Monday. Several Chinese military entities were among those receiving the exported equipment. The jury also convicted a Waltham, Massachusetts corporation, owned by one of the defendants, which procured the equipment from U.S. suppliers and then exported the goods to China through Hong Kong. The exported equipment is used in electronic warfare, military radar, fire control, military guidance and control equipment and satellite communications, including global positioning systems. The men were convicted of unlawfully exporting defense articles and Commerce controlled goods to China on numerous occasions between 2004 and 2007, and conspiring to violate U.S. export laws over a period of 10 years. They were also both convicted of filing false shipping documents with the Commerce Department. In addition, one of the defendants was convicted of immigration fraud for presenting a U.S. Permanent Resident Card, which she knew had been procured by making false and fraudulent statements to immigration officials, to enter the country.
Source: http://www.justice.gov/opa/pr/2010/May/10-nsd-580.html

21. *May 15, Arizona Daily Star* – (National) **Army formally cancels missile program.** The Army has formally canceled the Non-Line of Sight-Launch System, a billion-dollar missile program under development by Tucson, Arizona-based Raytheon Missile Systems and Lockheed Martin. The Navy is still evaluating its options for the system, which it had been considering for use aboard a new line of coastal combat vessels. The modular system, known as NLOS-LS or simply NLOS, features 15 all-weather missiles in a common launcher that can be mounted on an array of military vehicles. The NLOS-LS was part of the Army's Future Combat Systems program, which was canceled last year. Raytheon makes the NLOS-LS's Precision Attack Missile (PAM) and Lockheed Martin makes the launch unit, under a joint venture called Netfires LLC. "It's disappointing that the U.S. Army has decided to cancel the NLOS-LS program," Raytheon said in a prepared statement to the Star. "After a more than $1 billion investment over ten years, the program stands at 92 percent complete."

The cancellation comes after recent test failures and an examination of the program by a Pentagon review board, which recommended cancellation last month. The missile failed in four of six flights in a critical Army "limited user test" at White Sands Missile Range in New Mexico in late January and early February. The missile had succeeded in 12 of 17 prior tests, and Raytheon said the recent problems have been fixed.
Source: http://azstarnet.com/business/local/article_27505ee7-bcb2-5fb4-a5bb-6ee1a9cde68e.html

[Return to top]

Banking and Finance Sector

22. *May 19, SC Magazine* – (National) **US regulators form plans to encourage banks to better protect customers from online fraud.** A panel of regulators in the U.S. are drafting plans to force banks to protect their customers better from a surge in online account fraud. According to a report in the Financial Times (FT), a panel with representatives from the FDIC, the Federal Reserve System and other agencies is reacting to the rapid evolution of malicious computer programs designed to drain accounts. Among its plans is to require financial institutions to contact customers through means beside the Internet, following European banks actions in placing calls to clients' mobile phones to ensure that they intend to transfer money. The FT report also claimed that banks were warned in 2005 not to rely merely on user names and static passwords, which has led to U.S. institutions adopting two-factor authentication for big depositors. However, directives from the FDIC and others have allowed banks to skip that step if they had multiple layers of security checks to flag suspicious money movement.
Source: http://www.scmagazineuk.com/us-regulators-form-plans-to-encourage-banks-to-better-protect-customers-from-online-fraud/article/170494/

23. *May 19, Australian Broadcasting Corporation* – (International) **Anarchist group threatens G20 summit.** A Canadian anarchist group has claimed responsibility for a firebomb attack in Ottawa on the country's largest commercial bank, and is threatening to disrupt next months' G8 and G20 summits in Ontario. In a statement after the attack, a self-proclaimed group of anarchists said the Royal Bank was targeted because it was a sponsor of the Vancouver Olympic Games, which the group claims was held on stolen indigenous land. They also say the Royal is a major backer of Alberta's tar sands, which they describe as one of the most destructive industrial projects in human history. The statement was posted on a Web site along with a video showing the attack on the bank. The group has vowed to take their protest to Ontario for the G8 and G20 summits, where they say decisions will be made to further exploit people and the environment.
Source: http://www.abc.net.au/news/stories/2010/05/19/2904191.htm?section=justin

24. *May 18, Marketwatch* – (National) **Schapiro: SEC may push for market circuit-breakers.** The Securities & Exchange Commission chairwoman said May 18 she expects her agency to issue preliminary findings on its inquiries into the "flash crash"

on May 6, when the Dow Jones Industrial Average plunged nearly 1,000 points. Speaking via a video link to the CFA Institute's 2010 Annual Conference in Boston, the chairwoman said that her agency, in conjunction with the Commodity Futures Trading Commission, has been "looking at a number of issues that can be remediated quickly, even before the exact cause of the crash is known." Among the likely recommendations, she said is the implementation of circuit-breakers or "speed bumps" that give stocks "the opportunity to pause throughout all markets."
Source: http://www.marketwatch.com/story/schapiro-sec-may-push-for-market-circuit-breakers-2010-05-18

25. *May 18, Krebs on Security* – (International) **Fraud bazaar carders.cc hacked.** Carders.cc, a German online forum dedicated to helping criminals trade and sell financial data stolen through hacking, has itself been hacked. The once-guarded contents of its servers are now being traded on public file-sharing networks, leading to the exposure of potentially identifying information on the forum's users as well as countless passwords and credit card accounts swiped from unsuspecting victims. The breach involves at least three separate files being traded on Rapidshare.com: The largest is a database file containing what appear to be all of the communications among nearly 5,000 Carders.cc forum members, including the contents of private, one-to-one messages that subscribers to these forums typically use to negotiate the sale of stolen goods. Another file includes the user names, e-mail addresses and in many cases the passwords of Carder.cc forum users. A third file — which includes what appear to be Internet addresses assigned to the various Carders.cc users when those users first signed up as members — also features a breezy explanation of how the forum was compromised. The top portion of this file includes an oblique reference to the party apparently responsible for the Carders.cc site compromise, noting that the file is the inaugural issue of Owned and Exposed, no doubt the first of many such "e-zines" to come from this group. The leaked database contains no small amount of password and banking information for many innocent victims. In addition, these types of vigilante attacks typically come with hidden cost: For one thing, while it may be true that law enforcement officials could use some of this information to locate people engaged in computer trespass, and in buying or selling stolen personal and financial data, the public release of this information could just as easily prompt those individuals to abandon those accounts and Internet addresses, and even potentially jeopardize ongoing investigations.
Source: http://krebsonsecurity.com/2010/05/fraud-bazaar-carders-cc-hacked/

26. *May 18, ComputerWorld* – (National) **Smart credit cards arrive in U.S. — finally.** Credit cards featuring smart-card technology have been standard fare around the world for several years now — but not in the U.S., where financial institutions have continued using cards based on less-secure magnetic stripe technology. That may finally be about to change. Last week, the United Nations Federal Credit Union (UNFCU) became the first financial institution in the U.S. to unveil plans to issue credit cards that comply with the Europay MasterCard Visa (EMV) smartcard standard. The credit union's new Platinum Visa EMV cards will be issued to about 5,000 of its most high-value customers and can be used anywhere EMV cards are accepted. Cards

based on the EMV standard use an embedded microprocessor instead of a magnetic stripe to store cardholder data and all of the other information needed to use the card for a transaction. Many financial institutions that issue EMV Chip cards also require cardholders to enter a Personal Identification Number (PIN) as an added security measure when using the card. Chip-and-PIN credit cards are considered to be significantly safer than cards with magnetic stripes, which has led to the widespread adoption of EMV smartcards across Europe and in several other countries. EMVCo, an organization run by MasterCard, Visa, American Express and others to administer the EMV standard, estimates that close to a billion EMV cards were in use worldwide in 2009.
Source:
http://www.computerworld.com/s/article/9176936/Smart_credit_cards_arrive_in_U.S._finally

27. *May 18, Help Net Security* – (International) **Phishing page steals prepaid debit card account information.** Many people do not have a regular or a big enough income to receive a debit card, but would still like to have one since it can be really handy when settling bills or shopping online. The answer to this problem? Prepaid debit cards. The good thing about this option is that if card information is stolen and misused by cyber criminals, the monetary loss is limited to the (usually) small amount of money one has in one's account. Since these cards are regularly used by low- to mid-income citizens, who really can not afford to lose even that amount, Symantec's revelation that there are phishing sites out there that are posing as the main Web site of a well-known prepaid debit-card service will provide an almost lifesaving warning. The phishing site notifies the users that their account has been limited, and requires them to enter confidential information in order to re-activate the account. The inserted data is now in possession of the fraudsters behind this scheme, and it can be used to clean out the account. The pages' URL is randomly changed to avoid anti-phishing detection, but they are hosted on the same set of Internet Protocol addresses. According to Symantec, the attack method was prominent during the first half of May.
Source: http://www.net-security.org/secworld.php?id=9306

28. *May 17, Chicago Sun-Times* – (Chicago) **FBI offers $10K reward for info on 'Citibank Bandit'.** The FBI is offering a reward of up to $10,000 for information about the "Citibank Bandit," responsible for the robbery of 11 banks, six of which were Citibank branches, in and around the downtown Chicago area since February 2009. The most recent incident was an attempted robbery on January 29 at the Midwest Bank branch at 500 W. Monroe. According to witnesses, the robber entered the bank, announced a robbery and handed the teller a note claiming to be armed with a weapon and threatening harm if his demands for cash were not met. The teller turned her back on the robber, and when she turned back, both he and the note were gone, a release from the FBI said. No shots were fired in any of the robberies and no injuries were reported.
Source: http://www.myfoxchicago.com/dpp/news/metro/citibank-bandit-fbi-reward-20100517

For another story, see item **69**

[Return to top]

Transportation Sector

29. *May 19, Truckinginfo.com* – (Tennessee) **Emergency repairs get underway on I-24 sinkhole.** A large sinkhole opened up in the eastbound lanes of Interstate 24 near the Grundy/Coffee County line in Tennessee Tuesday. The Tennessee Department of Transportation said emergency repairs are now underway, and it expects the repairs to be finished by May 22. Tuesday afternoon, TDOT awarded a $267,000 contract to Highways Inc. to repair the damage immediately. The sinkhold is located between mile marker 127 and Exit 127 and is estimated to be 25-feet wide and 25-feet deep. The state will be detouring traffic off I-24 at Exit 114 to Highway 41 then to State Route 50 and back onto I-24 at Exit 127.
Source: http://www.truckinginfo.com/news/news-detail.asp?news_id=70466

30. *May 18, Associated Press* – (Wyoming) **Train derails for 2nd time in Wyoming.** A train that wrecked last week in the Wind River Canyon derailed for a second time in Cheyenne, Wyoming during its trip from Montana to Denver. A Burlington Northern-Santa Fe Corporation (BNSF) spokesman said five freight cars derailed Monday afternoon as the train was switching tracks from the Cheyenne yard to the main line. He said the cars didn't spill any freight and there were no injuries. The line reopened Tuesday morning. The same train derailed May 12 about five miles south of Thermopolis in central Wyoming, resulting in the spillage of diesel fuel, bentonite clay and barley. BNSF removed the wrecked locomotives and cars, repaired the damaged track and reopened the line near Thermopolis on Saturday.
Source: http://billingsgazette.com/news/state-and-regional/wyoming/article_31d31c8a-62ac-11df-8336-001cc4c002e0.html

31. *May 18, CNET News* – (California) **Navy enlists sea mammals to defend California ports.** The U.S. Navy is showing off some unlikely recruits in California. Its Marine Mammal Program conducted training exercises Tuesday in the San Francisco Bay using sea lions and dolphins that have been trained to perform underwater surveillance for object detection, location, marking, and recovery. In a full-scale regional exercise focusing on the state's response and recovery to multiple terrorist attacks at Bay Area ports, federal, state, and city officials took part in the Golden Guardian emergency preparedness program. At Pier 48 in San Francisco, the city's police and fire departments, along with its Emergency Operations Center, conducted a drill demonstrating the ability of dolphins and California sea lions to help protect coastal areas from maritime attacks.
Source: http://news.cnet.com/2300-11386_3-10003492.html?tag=mncol

32. *May 18, Tulsa World* – (Oklahoma) **Tulsa airport reenacts airplane crash disaster.** More than 100 emergency responders and dozens of fire trucks, ambulances and rescue vehicles participated in an aircraft crash disaster drill Tuesday at Tulsa

International Airport (TIA) in Tulsa, Oklahoma. The disaster exercise, part of the Federal Aviation Administration's (FAA) Part 139 requirements for TIA's certification as a commercial airport, began just after 9 a.m. and involved representatives from more than a dozen Tulsa agencies. Participating in the drill were representatives of the Tulsa Airport Authority, American Airlines, American Red Cross, city of Tulsa, EMSA, FAA, FBI, Oklahoma Air National Guard, Transportation Security Administration, Tulsa Area Emergency Management Agency, Tulsa County Sheriff's Office, Tulsa Fire Department and the Tulsa Police Department. The drill's script specified "Tri-State Airlines" Flight 2009, a "Boeing 777-200ER" with 299 passengers and a crew of five, was on final approach to the airport's 7,372-foot east-west crosswind runway when it encountered multiple bird strikes at 2,000 feet. For the training exercise, American Airlines supplied a Boeing MD-80 aircraft, whose capacity is between 139 and 172 passengers, depending on seating configuration. "We had no control over the type of plane provided to us as a tool for first responders to work around," said the marketing director for the Tulsa Airport Authority. "Our scenario called for a 777 because we wanted to test the response capabilities for a larger number of passengers."
Source:
http://www.tulsaworld.com/business/article.aspx?subjectid=45&articleid=20100518_45_0_brbrMo96770

33. *May 15, United Press International* – (Hawaii) **Hawaii air passenger busted for stun gun.** A federal judge in Hawaii agreed to let a Japanese citizen return home after a high-powered stun gun was found in his carry-on luggage. The man was arrested May 14 when he allegedly tried to board a plane in Honolulu with a 750,000-volt stun gun in his bag. "This was a great catch," an FBI special agent told the Honolulu Advertiser. "The bag screeners are to be commended." The man said he brought the stun gun with him on vacation for personal protection. It was packed in his checked luggage during the flight from Tokyo to the islands. The man was charged with attempting to bring a concealed weapon aboard an airliner. The Honolulu Star-Bulletin said the judge agreed to release him on a signature bond so he could fly back to Japan to attend a funeral. He will be due back in court May 28.
Source: http://www.upi.com/Top_News/US/2010/05/15/Hawaii-air-passenger-busted-for-stun-gun/UPI-63301273943480/

For more stories, see items **3**, **4**, **5**, and **6**

[Return to top]

Postal and Shipping Sector

See item **13**

[Return to top]

Agriculture and Food Sector

34. *May 19, WFTV 9 Orlando* – (Florida) **Wendy's customer chases workers with stun gun.** A drive-thru customer at a Daytona Beach, Florida Wendy's restaurant chased employees with a stun gun after not getting the packets of condiments she wanted, police said. The woman became irate May 17 at the Wendy's on LPGA Boulevard. Two women were arrested when police found them driving down the road less than one mile from the restaurant. Employees told WFTV the whole incident started with some yelling about condiments. It took a turn for the worst when one of the women allegedly came in brandishing a stun gun. Wendy's employees scattered when the woman, upset about what she didn't get at the drive-thru, rushed in firing the stun gun. "I went out the back door, the security door, and ran to 7-Eleven. They let me borrow a cell phone and I called in a description, 'cause I didn't know if it was a gun or not," an employee said. "Nobody got tased, but he was going to get tased if he didn't run all the way back," another employee said. The two women were arrested and are facing charges of assault with a deadly weapon and principle to assault.
Source: http://www.wftv.com/news/23579965/detail.html

35. *May 19, Marco Eagle* – (Florida) **Six Immokalee tomato vendors cited for violating food-safety rules.** Six tomato vendors at a road-side farmer's market in Immokalee have been cited for violating Florida's food safety rules. The vendors face misdemeanor charges for not properly sanitizing and packing tomatoes. The violations were discovered May 17 during a sweep by regulatory inspectors and law enforcement officers with the Florida Department of Agriculture and Consumer Services at a market off New Market Road. The new safety rules were enacted in 2008. Last year, the Department of Agriculture did sweeps, but only gave out warnings, said an agency spokesman. "Those were like the dress rehearsals," he said. Now, enforcement is getting tougher. "We plan on visiting all kinds of places," the spokesman said. The vendors in Immokalee will have to appear in court. A misdemeanor conviction can carry a sentence of up to six months in jail, and fines as high as $5,000, the spokesman said. "I don't know that anyone would advocate jail time for anyone here," he said. "But when you issue rules, if they are going to mean anything, you've got to enforce them." The new rules require that tomatoes are sanitized to reduce microbial contamination and harvested into plastic boxes.
Source: http://www.marconews.com/news/2010/may/18/six-immokalee-tomato-vendors-cited-violating-food-/

36. *May 18, WPSD Local 6 Paducah* – (National) **Toxic chemical found in canned foods.** Eating common canned foods is exposing consumers to levels of bisphenol A (BPA) equal to levels shown to cause health problems in laboratory animals, according to a new study released today by Illinois PIRG and the National Work Group for Safe Markets, a coalition of public health and environmental groups. The study tested food from 50 cans from 19 U.S. states and one Canadian province for BPA contamination. Over 90 percent of the cans tested had detectable levels of BPA, some at higher levels than have been detected in previous studies. The new study comes as Illinois lawmakers in Springfield consider legislation to eliminate BPA from baby-food packaging. The canned foods tested were brand name fish, fruits, vegetables, beans, soups, tomato products, sodas and milks. The cans were purchased from retail stores

and were chosen from report participants' pantry shelves, and sent to an independent laboratory for testing. One can of DelMonte green beans had the highest levels of BPA ever found in canned food, at 1,140 parts per billion. The test results show there is no consistency in the amount of BPA in specific food brands or in types of food, which prevents consumers from being able to avoid BPA canned foods just by looking at a label. For example, two different cans of the same brand of peas with two separate "lot numbers" were drastically different: one had six parts per billion of BPA, while the other had over 300 parts per billion of BPA. "Anyone who reads this report would agree that getting BPA out of food is an urgent food safety issue that demands immediate congressional action," said the policy director at the Breast Cancer Fund.
Source: http://www.wpsdlocal6.com/news/local/94182714.html

37. *May 18, Washington Post* – (National) **Pre-cut lettuce is suspected cause of food poisoning outbreak.** Bagged lettuce suspected of causing a multi-state outbreak of E. coli illness raises new questions about whether pre-cut produce is riskier than whole vegetables. The outbreak, which involves romaine lettuce cut up and distributed in bags to 23 states and the District, is the latest in a string of recent food-poisoning cases involving pre-shredded leafy greens. The romaine in question was not sold directly to consumers in the produce section but was used by food service companies and supermarkets in salad bars and "grab and go" meals. It is difficult to judge whether pre-cut produce has been linked to more outbreaks than whole vegetables because state and federal health officials don't always specify whether the leafy greens associated with an outbreak were bagged or whole. A senior adviser for produce safety at the Food and Drug Administration said bagged greens represent a disproportionate number of recalls, chiefly because they're easier to identify than whole produce. But, he said, pre-cut produce is not inherently riskier than whole vegetables. The current outbreak is drawing special attention because the romaine lettuce was contaminated with E. coli O145, a strain that is primarily found in cattle and wildlife feces and has never before been linked to a food-borne illness, according to the CDC. The chief of CDC's Enteric Diseases Epidemiology branch said it is likely that E. coli O145 has caused previous food poisonings but has gone undetected because only about 5 percent of clinical laboratories are able to detect it.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/05/17/AR2010051703033.html?hpid=sec-health

38. *May 18, United Press International* – (National) **Method found to stop E. coli in cattle.** U.S. microbiologists said they have identified a process that might be able to help prevent outbreaks of a food-borne illness caused by E. coli in cattle. Scientists at the University of Texas Southwestern Medical Center, working with the U.S. Department of Agriculture, said they interfered with a genetic sensing mechanism that allows the E. coli strain known as enterohemorrhagic O157:H7, or EHEC, to form colonies within cattle, causing the bacteria to die before reaching the animals' recto-anal junction — the primary site of colonization. Most other strains of E. coli gather in the colon. "We're diminishing colonization by not letting EHEC go where it needs to go efficiently," said an associate professor of microbiology and senior author of the study. "If we can find a way to prevent these bacteria from ever colonizing in cattle, it's

possible that we can have a real impact on human disease." She said the finding is important because an estimated 70 percent to 80 percent of U.S. cattle herds carry EHEC. Although EHEC can be a deadly pathogen to humans, the bacterium is part of cattle's normal gastrointestinal flora. The findings are to be reported in the Proceedings of the National Academy of Sciences.
Source: http://www.upi.com/Science_News/2010/05/18/Method-found-to-stop-E-coli-in-cattle/UPI-54321274194978/

39. *May 18, Anchorage Daily News* – (National) **At least 20 report stomach woes after Rotary luncheon.** The Anchorage, Alaska health department is investigating complaints that 20 or more people suffered from stomach illness after the Anchorage Downtown Rotary Club luncheon at the Dena'ina Civic and Convention Center last Tuesday, May 11. Early indications are that under-cooked fiddlehead ferns might be implicated, but the city is surveying everyone who attended to find out what they ate and who got sick, said the city food-safety program manager. The Rotary Club president said roughly 110 people attended the lunch. The food-safety program manager said some employees at the convention center also ate the food after the luncheon. Some had severe cramps and diarrhea, but all of the people whom city officials have talked to so far recovered fairly quickly, he said. The buffet included chicken, beef with a sauce, cooked vegetables and tossed vegetables as well as the fiddlehead ferns, said the food-safety program manager. None of the items except the ferns were handled in a way that would suggest a problem, he said. If the culprit turns out to be something other than ferns, the city might be able to test the food item for toxins, he said. But if it is not the ferns, not enough is known about any potential toxins to test for, he said. Because the ferns are suspected, the city is working with the federal Food and Drug Administration, and is tracing their origin. The ferns came from a British Columbia producer, were shipped to a warehouse in Encino, California, and then made their way to a supplier in Anchorage.
Source: http://www.adn.com/2010/05/17/1281986/at-least-20-report-stomach-woes.html

For another story, see item **71**

[Return to top]

Water Sector

40. *May 19, Naperville Sun* – (Illinois) **City responding to chlorine leak.** Naperville, Illinois fire officials responded to a minor chlorine leak Wednesday morning at the city's water treatment plant at 3612 Plainfield-Naperville Road. "There is no danger to citizens at this time," said the deputy fire chief at 9:40 a.m., about 15 minutes after the leak was called in by a city employee. "It's a minor leak right now. We have our fire department haz-mat team on the scene working to contain the leak." The leak was coming from one of the cylinders that contains chlorine used in the water-treatment process. "This is a small, 150-pound cylinder of gaseous chlorine," the deputy fire chief said. No evacuation was required. Seven fire department units in all — two of which

make up the hazardous-materials team — responded to the incident.
Source:
http://www.suburbanchicagonews.com/napervillesun/news/2292318,Naperville-chlorine-leak-NA0519810.article

41. *May 19, MetroWest Daily News* – (Massachusetts) **Framingham orders General Chemical to clean contaminated water tank.** Framingham, Massachusetts issued a cease-and-desist order May 19 against General Chemical Corp. following the discovery of toxins in a water tank connected to the municipal water supply. There are back-flow prevention measures in place, and the assistant fire chief said there is currently no threat to public health. But fire department and town officials are concerned. General Chemical found that a 180,000-gallon storage tank at its Southside facility, kept full for fire protection, somehow became tainted. "We do not know exactly just how yet," he said. Officials at the hazardous waste transfer site notified the town and state Department of Environmental Protection (DEP) last week after testing. The cease-and-desist order was then jointly issued May 18 by the fire and building departments and hand-delivered to the company. It requires General Chemical, 133 Leland St., to work with the DEP to figure out the best way to get rid of the contaminants and clean the tank. The company has been under scrutiny in recent weeks, and the board of health is planning to hold a public hearing to determine whether the company needs to be run under tighter regulations or possibly shut down.
Source: http://www.metrowestdailynews.com/top_stories/x1234246822/Framingham-orders-General-Chemical-to-clean-contaminated-water-tank

42. *May 18, U.S. Environmental Protection Agency* – (Illinois) **EPA cites Sharp Homes-Hunter's Ridge Development for violation of federal stormwater regulations.** U.S. Environmental Protection Agency Region 5 has issued a complaint and final order against Sharp Homes-Hunter's Ridge Development for failure to comply with federal stormwater rules. The complaint cites the Joliet, Illinois, company for failing to prevent or minimize discharges, initiate stabilization measures, conduct inspections, and maintain proper records. A penalty of $15,000 has been assessed. Construction on more than five acres of land being developed for homes allegedly caused discharges of stormwater through sewers, surface runoff and discharge pipes to Aux Sable Creek, a tributary to the Illinois River. Procedures for erosion control, as required by a National Pollutant Discharge Elimination System, were not followed.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/7DDF1B1AD6E4A06285257727006E198A

43. *May 18, United States Department of Justice* – (Missouri) **Kansas City, Missouri to spend $2.5 billion to eliminate sewer overflows.** The city of Kansas City, Missouri, has agreed to make extensive improvements to its sewer systems, at a cost estimated to exceed $2.5 billion over 25 years, to eliminate unauthorized overflows of untreated raw sewage and to reduce pollution levels in urban storm water, the Justice Department and U.S. Environmental Protection Agency announced Monday. The settlement, lodged in federal court in Kansas City, requires the city to implement the overflow-control plan,

which is the result of more than four years of public input. The plan is designed to yield significant long-term benefits to public health and the environment, and provide a model for the incorporation of green infrastructure and technology toward solving overflow issues. When completed, the sanitary sewer system will have adequate infrastructure to capture and convey combined stormwater and sewage to treatment plants. This will keep billions of gallons of untreated sewage from reaching surface waters.
Source: http://www.justice.gov/opa/pr/2010/May/10-enrd-584.html

44. *May 18, KCBY 11 North Bend* – (Oregon) **Coquille water could be contaminated.** Coquille, Oregon residents are being warned to boil their tap water before consumption after most residents lost water supply Monday. Millions of gallons of water were drained into a field on 10th Street in Coquille late Sunday through Monday morning, causing a loss of water supply. According to a press release from the Public Works Department, the lack of water pressure in the lines could potentially bring harmful bacteria, such as Fecal Coliforms and E. Coli from human or animal waste. The City of Coquille is currently collecting water test samples throughout the system and say they expected to have the results by Wednesday afternoon.
Source: http://www.kcby.com/news/local/94206344.html

45. *May 18, Pioneer Press* – (Illinois) **Potential hazmat situation averted.** A hazardous materials leak in Wilmette, Illinois last week flowed into the sewer system and threatened to pollute the area's water supply. About 75 gallons of diesel fuel spilled in front of a home at 7:24 a.m. May 12 on the 200 block of 15th Street. The Wilmette Fire Department responded to the leak and, along with a private contractor, cleaned the site over a five-hour span, according to the fire chief. "The truck was dropping off materials at a home that was being built at 225 15th St.," he said. "The truck was pulling out and there was a fence post ... on the ground. As it ran over it, it pierced the diesel tank." His team estimated that 25 to 30 gallons of fuel got into the sewer system. The leak was caught in two catch basins before it could enter a combined storm and sanitary sewer that would have led to a Metropolitan Water Reclamation District treatment facility, according to a supervisor with the district. The leak was immediately reported to the Illinois Emergency Management Agency, the Illinois Environmental Protection Agency, and the water reclamation district.
Source: http://www.pioneerlocal.com/wilmette/news/2289402,wilmette-hazmat-052010-r1.article

46. *May 18, Nashville Business Journal* – (Tennessee) **Nashville faces $200 million in water, sewer system damages.** Damages to Nashville's water and sewer system total $200 million, according to credit analysis released Tuesday by Standard & Poor's. Metro government also expects to lose $3.9 million in hotel and motel revenues over six months and has allocated $10 million for debris cleanup, according to a credit analyst. The information was included in a report that summarized damages to 16 Tennessee cities and counties affected by flood damage earlier this month. Standard & Poor's will not alter its credit ratings on any of the local governments. "Any decline in assessed value or sales tax revenue is expected to be temporary and will be more than

offset by federal funding," the report states. Damage estimates are based on figures provided by city and county officials. Most costs will be reimbursed, according to the report. In the case of Nashville, unreimbursed costs are expected to total $3 million for general government and $25 million for Metro Water Services. Metro government has $47.3 million in unrestricted reserves, which equals about 6.6 percent of its operating budget. Damages to Metro Water Services include those to the K.R. Harrington Water Treatment Plant, which was submerged in the flooding. The flood contaminated the plant and destroyed electrical systems and computerized monitoring systems. Water conservation has been urged as it is expected the city will have to solely rely on its other treatment plant — for about a month.
Source: http://www.bizjournals.com/nashville/stories/2010/05/17/daily18.html

47. *May 17, U.S. Geological Survey* – (National) **Instant information about water conditions: Ask the river to text you a WaterAlert.** Now one can receive instant, customized updates about water conditions by subscribing to WaterAlert, a new service from the U.S. Geological Survey (USGS). Whether one is watching for floods, interested in recreational activities or concerned about the quality of water in one's well, WaterAlert allows one to receive daily or hourly updates about current conditions in rivers, lakes and groundwater when they match conditions of concern. WaterAlert allows users to receive updates about river flows, groundwater levels, water temperatures, rainfall, and water quality at any of more than 9,500 sites where USGS collects real-time water information. This information is crucial for managing water resources, including during floods, droughts, and chemical spills. WaterAlert also allows kayakers, rafters and boaters to better understand when conditions are optimal and safe for recreational activities. WaterAlert users start at http://water.usgs.gov/wateralert and select a specific site. Users then select the preferred delivery method (email or text), whether they want hourly or daily notifications, which data parameter they are interested in, and the threshold for those parameters. Users can set the system to alert them when conditions are above a value, below a value, and between or outside of a range.
Source: http://www.usgs.gov/newsroom/article.asp?ID=2464

For another story, see item **10**

[Return to top]

Public Health and Healthcare Sector

48. *May 19, Homeland Security NewsWire* – (Utah) **Utah implements harsh triage guidelines for bioterror, epidemic emergencies.** Utah's new triage health emergency guidelines would see some children and some seniors turned away from hospitals during a bioterror or epidemic emergency; those who are severely burned, have incurable and spreading cancer, fatal genetic diseases, end-stage multiple sclerosis, or severe dementia will be turned away; people older than 85 also would not be admitted in the worst pandemic; those who have signed "do not resuscitate" orders could be denied a bed. When a killer flu strikes, with several thousand sick or injured and no

room to spare in understaffed hospitals, care will be denied to the sickest adults and children. Those who are severely burned, have incurable and spreading cancer, fatal genetic diseases, end-stage multiple sclerosis, or severe dementia will be turned away. They can be sent elsewhere for comfort care, such as painkillers, but they will not be treated for the flu, according to controversial Utah triage guidelines being modeled across the country. People older than 85 also would not be admitted in the worst pandemic. Those who have signed "do not resuscitate" orders could be denied a bed. Doctors could remove ventilators from patients deemed unlikely to recover, to give them to other patients.
Source: http://homelandsecuritynewswire.com/utah-implements-harsh-triage-guidelines-bioterror-epidemic-emergencies

49. *May 18, CNN* – (National) **FDA widens Tylenol probe.** The Food and Drug Administration (FDA) said Monday it is expanding its investigation of a Johnson & Johnson manufacturing division tied to the recent recall of children's drugs. On May 1, Johnson & Johnson's McNeil Consumer Healthcare unit recalled some 50 children's versions of non-prescription drugs, including Tylenol, Motrin and Benadryl. Then on May 6, the FDA issued a scathing 17-page inspection report of McNeil's Fort Washington, Pennsylvania, plant that produced the drugs. Now the FDA is conducting a companywide investigation of McNeil's "manufacturing practices to determine whether similar problems exist throughout the company and what additional steps the agency must take to ensure that these problems do not recur," according to a statement posted Monday on the FDA Web site. In a statement e-mailed to CNNMoney Monday, McNeil said the company "is conducting a comprehensive quality assessment across its manufacturing operations and continues to cooperate with the FDA." Johnson & Johnson, which subsequently shut the Fort Washington facility, has declined to disclose what other products are manufactured at the plant.
Source: http://money.cnn.com/2010/05/17/news/companies/mcneil_fda_investigation/

50. *May 18, Global Security Newswire* – (National) **U.S. stockpile receives new smallpox vaccine.** The U.S. Strategic National Stockpile is now receiving shipments of a modified smallpox vaccine intended for people who have a compromised immune system and would not be able to safely receive the usual treatment, the Center for Infectious Disease Research and Policy reported May 17. The standard smallpox vaccine contains a live vaccinia virus that in a few cases can lead to serious health effects. The Imvamune vaccine is made from a less-potent version of the virus that is unable to duplicate itself and spread in humans. Though smallpox has been eradicated in nature, there are worries that the often lethal disease could be used in an act of biological terrorism. The U.S. government has procured sufficient quantities of the standard smallpox vaccine to safeguard all U.S. citizens should such an attack occur.
Source: http://www.globalsecuritynewswire.org/gsn/nw_20100518_3997.php

For another story, see item **69**

[Return to top]

Government Facilities Sector

51. *May 19, Congress.org* – (National) **Immigration groups escalate tactics.** Immigrant-rights groups say they are stepping up their tactics to prompt action from Congress on immigration. They are planning to block buses leaving deportation centers, stage sit-ins in lawmakers' offices, and protest companies doing business in Arizona. Those actions in Seattle, Los Angeles, New York and Washington, D.C. will culminate May 29, when groups from across the nation will gather in Arizona for a protest. Many of those protest actions could result in arrests. Students were arrested in Arizona Monday while protesting at an Arizona Senator's office and are expected to face deportation hearings. "Many more will step forward to put their bodies on the line in the weeks to come," an official with the Center for Community Change said on a conference call with reporters Tuesday. He emphasized that none of the planned activities will be violent. The May 29 protest coincides with events being planned by conservative and tea party groups.
Source: http://www.congress.org/news/2010/05/18/immigration_groups_escalate_tactics

52. *May 18, WSBTV 2 Atlanta* – (Georgia) **Peachtree suspicious package deemed harmless.** Peachtree Street in downtown Atlanta was shut down Tuesday evening after someone reported a suspicious package. Atlanta police said an envelope containing some type of powder was delivered to the 15th floor at No. 2 Peachtree. The 42-story building houses state offices. A fire department representative told a Channel 2 Action News reporter that the package was sent to the public health department. Haz-mat crews analyzed the package and deemed it harmless.
Source: http://www.wsbtv.com/news/23597129/detail.html

53. *May 18, OPB News* – (Washington) **Draft federal report on Beryllium at Hanford released to limited audience.** Some people sickened by beryllium said the toxic metal is finally getting adequate attention at the Hanford Nuclear Reservation in Hanford, Washington. The Department of Energy (DOE) has completed a long awaited report on workers' exposure to beryllium. But a correspondent reports the document has not yet been made public. Beryllium is a light-weight metal that was used to seal radioactive rods. In fine particles it can get into the lungs. A former worker at Hanford was diagnosed with Chronic Beryllium Disease more than 10 years ago. Since then he has been warning of the dangers of beryllium, but he said he was ignored. Now a federal investigation has resulted in a 100-page draft report by the DOE's Office of Health Safety and Security. The former worker was one of the few people who were allowed to see it this week. He said he thinks the findings could have been more critical of Hanford managers. But he noted the issue has reached a tipping point.
Source: http://news.opb.org/article/7365-draft-federal-report-beryllium-hanford-released-limited-audience/

54. *May 17, Nextgov* – (National) **IG: Poor controls over access to IRS portal put taxpayer data at risk.** The Internal Revenue Service (IRS) failed to implement adequate security measures to protect sensitive data that tax professionals entered into a Web portal, according to an inspector general (IG) report released Monday. A fiscal

2009 audit by the Treasury IG for Tax Administration showed tax professionals were able to transfer authorization to access the Registered User Portal to individuals who did not go through the standard checks for tax compliance, past violations of e-file requirements and criminal records. The IRS performs suitability checks when tax firm principals or officials apply for entry, but then allows them to delegate their access rights to others by filing for power of attorney, auditors found. "Taxpayers expect the IRS to protect their personal data, and we believe the power of attorney document does not provide the same assurance as the suitability check," the IG stated. "Any individual can become a delegated user. Many of the delegated users may have questionable backgrounds." The audit found there were 9,988 delegated users permitted to file income-tax returns electronically through the portal. About 6,500 of them also had access to electronic services that enabled them to retrieve and manipulate taxpayer data. In addition, the IRS allows authorized users to assign a special principal consent privilege to a delegated user, which lets that user extend his or her privileges to others.
Source: http://www.nextgov.com/nextgov/ng_20100517_2540.php

For another story, see item **6**

[Return to top]

Emergency Services Sector

55. *May 19, Asheville Citizen-Times* – (North Carolina) **Graham County Sheriff Russell Moody calls fire at HQ suspicious.** Graham County, North Carolina government workers conducted business by mobile phone for a second day Tuesday after a fire damaged the county's communication system. The sheriff also on Tuesday called the fire suspicious and said investigators had developed leads in the case. The state bureau of investigation is handling the inquiry into the blaze, which happened about 2:30 a.m. Monday. The fire gutted a concrete block office building on the side of the sheriff's office that housed two offices for the department's four detectives. Smoke and heat damage was spread through the one-story structure, which includes the county telephone system. County phone service could be restored today. The sheriff said it is still unclear how much, if any, criminal evidence was lost in the fire. He said most of the evidence is stored in a vault in the other side of the building. Detectives stored some evidence in smaller safes in their offices. The computers in the investigations office were destroyed. The county manager said Tuesday the damage would be less than the first estimate of $1 million. Some computers elsewhere in the sheriff's office might be salvageable, she said.
Source: http://www.citizen-times.com/article/20100519/NEWS/305190030

56. *May 19, Natchez Democrat* – (Louisiana) **FBI, ATF investigate Vidalia Police Department.** Agents from the Federal Bureau of Investigation and the Bureau of Alcohol, Tobacco, Firearms and Explosives were on the scene at the Vidalia, Louisiana Police Department Tuesday as part of an unspecified criminal investigation. The Louisiana State Police were also present at the police station. Just before 10 a.m., things in the department appeared normal, with officers booking in a suspect and others

discussing current events in the assistant chief's office. By the end of the hour, however, the outside federal and state officials had restricted access into the police station and were searching vehicles in the parking lot. The outside agents had left the station by Tuesday afternoon, and the department was properly functioning and had continued to properly function throughout the day Tuesday, and that Tuesday evening even the chief was out doing patrols. "The residents' safety has not been in jeopardy, (the police) are doing the patrols and they are still answering calls," the Vidalia mayor said.
Source: http://www.natchezdemocrat.com/news/2010/may/19/fbi-atf-investigate-vidalia-police-department/

57. *May 18, Nextgov* – (National) **Bill would require FBI to fill in gaps in criminal records database.** A bill introduced in the U.S.House of Representatives would strengthen the accuracy of the FBI's criminal records database by requiring the U.S. Attorney General's Office to verify that crime data is up to date. Employers rely on the database to conduct background checks on potential hires. The 2010 Fairness and Accuracy in Employment Background Checks Act would require the Attorney General to find out from court offices, including those in state and local jurisdictions, the outcome of arrests whenever an employer requests a background check, and update that record in the National Crime Information Center database. In cases where the Attorney General discovers an arrest was dismissed in court, he has 10 days to update the record before responding to the employer's request. Employers often consult the NCIC database to conduct background checks on individuals applying for jobs in law enforcement, homeland security or organizations where they would be working with vulnerable populations, such as children and the elderly. Typically only public sector entities can request FBI background checks, though certain private sector companies — such as those supporting federal homeland security efforts — can as well.
Source: http://www.nextgov.com/nextgov/ng_20100518_2029.php?oref=topnews

For another story, see item **68**

[Return to top]

Information Technology Sector

58. *May 19, Network World* – (International) **Nanotech will be focus for future criminal hackers.** Criminal hackers once rejoiced in manipulating the new digital phone systems in the 1960s and 1970s; then they moved on to using modems and hacking into mainframes in the 1970s and 1980s; then they exploited the new local area network technology and the burgeoning Internet in the 1980s. Malware writers moved from boot-sector viruses on floppy disks in the 1980s to file-infector viruses and then to macro viruses in the 1990s and vigorously exploited worms and Trojans for botnets in the recent decade. So what's next on the horizon? Recently a report in the "Random Samples" column by a contributor to SCIENCE magazine for Feb. 19, 2010 (Vol 327, p 927) told of the fuss in France "over the pros and cons of nanotechnology." Apparently in late January 2010, "the committee organizing the series of 17 debates

threw in the towel, replacing the final two meetings with 'Internet workshops' and making the wrap-up event in Paris on 23 February by invitation only." The changes were the result of "heckling by antinanotech protesters in five cities." The question remains, however, of whether the agents of change are and will be taking the lessons of information security into account as they explore the possibilities of new technology. For example, the nanoparticles called polyamidoamine dendrimers (PAMAM) "cause lung damage by triggering a type of programmed cell deathâ ¦." The anti-nanotech organization NANOCEO (Nanotechnology Citizen Engagement Organization) has an enormous list of articles and scientific reports about the potential environmental risks of nanotechnology.
Source: http://www.networkworld.com/newsletters/sec/2010/051710sec2.html

59. *May 19, Help Net Security* – (International) **Microsoft warns of flaw affecting 64-bit Windows 7.** A vulnerability in the Canonical Display Driver (cdd.dll) in 64-bit versions of Windows 7 and Windows Server 2008 R2, and Windows Server 2008 R2 for Itanium-based Systems, could allow remote code execution. "The Windows Canonical Display Driver does not properly parse information copied from user mode to kernel mode," states Microsoft in a security advisory published May 19. "In most scenarios, an attacker who successfully exploited this vulnerability could cause the affected system to stop responding and automatically restart. It is also theoretically possible, but unlikely due to memory randomization, that an attacker who successfully exploited this vulnerability could run arbitrary code. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights." To take advantage of the vulnerability, the attackers would have to trick the user into viewing a "specially crafted image file with an affected application," likely hosted on a malicious Web site. To do that, it is likely that they would employ social engineering tactics such as sending an e-mail or an instant message containing the malicious link and purporting to be from a user's friend and with a link back to a curious/funny image, video, or test.
Source: http://www.net-security.org/secworld.php?id=9313

60. *May 19, The Register* – (National) **Man accused of DDoSing conservative talking heads.** Federal prosecutors have accused a man of carrying out a series of botnet offenses including attacks that brought down the Web sites of conservative talking heads. The suspect was an undergraduate student at the University of Akron in Ohio at the time of the distributed denial-of-service (DDoS) attacks, which lasted over a five-day period in March 2008, prosecutors alleged in court documents. The attacks on billoreilly.com, anncoulter.com and joinrudy2008.com "rendered each website inoperable, at least temporarily, and required intervention and repair by the owners of such sites, and caused damages or losses which exceeded $5,000," they wrote. The suspect, who went by the handle "FrostAie," also stands accused of using his botnet to launch a much bigger assault on a University of Akron server that knocked out the college's entire network, depriving "tens of thousands of students, faculty and staff members" of connectivity for more than eight hours. Prosecutors said the attack appeared to be a mistake and that the intended target was an unnamed gaming server that was hosted on the university network. The outage cost the university more than

$10,000. Prosecutors also accuse the suspect of using his botnet to steal credit card information. When agents raided the suspect's dorm room on March 28 2008, they allegedly retrieved almost 3,000 stolen log-in credentials, and 136 pieces of data for compromising card accounts.
Source: http://www.theregister.co.uk/2010/05/19/bill_oreilly_ddos_attacks/

61. *May 19, CSO* – (International) **Expert: Skype worm no cause for panic.** Security research firm Bkis earlier in May warned of a vicious virus targeting both Skype and Yahoo! Messenger. Bkis said in a blog post the attack involved inserting malicious URLs into chat windows with sophisticated social engineering hooks. Each time, the messages sent have different contents, noted Bkis researchers. Examples include "Does my new hair style look good? bad? perfect?" "My printer is about to be thrown through a window if this pic wont come our right. You see anything wrong with it?" The message contains a link to a Web page that appears to lead to a JPEG or image file. "The users are more easily tricked into clicking the link by these messages, because users tend to think that "their friend(s)" are asking for advice," Bkis said in its posting. "If a user clicks the link, his browser will immediately load to a website with Rapidshare-like interface, and a .zip file will be available for download." The W32.Skyhoo.Worm, as it was named by Bkis, automatically exits if the victim's computer is not installed with Skype or Yahoo! Messenger, and automatically sends messages with different contents containing malicious URLs to user names in the Skype/Yahoo! Messenger friend list of the user. The owner of the Web site skypetips.com and author of 'Skype Me! From Single User to Small Enterprise and Beyond ,' spoke to CSO earlier this year about Skype's benefits and challenges in the business environment. According to the owner and author it is not Skype's fault for this attack. Instead, the focus should be on awareness among users if they are using Skype in the workplace and they should be given a warning about social engineering rather than worrying about the application's security.
Source:
http://www.pcworld.com/article/196644/expert_skype_worm_no_cause_for_panic.html

62. *May 18, Websense* – (International) **Zeus is forwarding Adobe updates again.** Websense Security Lab ThreatSeeker Network has detected a new batch of malicious e-mails containing Zeus payloads. This campaign is very similar to another which Adobe reported on a couple of weeks ago. The social engineering tricks on this campaign have gotten considerably better. The messages appear to be forwarded from a director of information services who apparently received update instructions directly from an associate at Adobe. The message from the Adobe associate states that the update link is to patch CVE-2010-0193. There are two links in the message that lead to the same IP address hosting a PDF file for instructions and an executable that is meant to be the patch to apply. The executable file named adbp932b.exe (SHA1 0632f562c6c89903b56da235af237dc4b72efeb3) has minimal coverage of about 7 percent. The attackers sending these messages have taken their social engineering tactics even further with the executable file linked in the messages. There is a new executable hosted on the attacker's IP address (SHA1 7af53e5924b45ebcb48d8b17e20b66a5979600f3) which seems to behave like a typical

installer. There are even setup prompts and a EULA as one moves along in the installation but once the installation is complete, a backdoor is installed on the victim's computer. Because there is such a small amount of messages the fact that this installer is infecting with a backdoor, Websense believe this to be another targeted attack.
Source: http://community.websense.com/blogs/securitylabs/archive/2010/05/18/zeus-is-forwarding-adobe-updates-again.aspx

63. *May 18, IDG News Service* – (International) **Facebook fixing embarrassing privacy bug.** Facebook is fixing a Web programming bug that could have allowed hackers to alter profile pages or make restricted information public. The flaw was discovered last week and reported to Facebook by a senior security analyst with security firm Alert Logic. The bug has to do with the way that Facebook checked to make sure that browsers connecting with the site were the ones they claimed to be. Facebook's servers use code called a "post_form_id" token to check that the browser trying to do something — liking a group, for example — was actually the browser that had logged into the account. Facebook's servers check this token before making any changes to the user's page, but the analyst discovered that when he simply deleted the token from messages, he could change many settings on any Facebook account. Facebook worked with Alert Logic to fix the bug, known as a cross-site request forgery (CSRF), a Facebook spokesman confirmed in an e-mail message. "It's now fixed," he said. "We're not aware of any cases in which it was used maliciously." But as of late afternoon May 18 after the spokesman sent his e-mail, Facebook had not completely fixed the issue. For testing purposes, the researcher created a Web page with an invisible iFrame HTML element that he programmed in Javascript. When the IDG News Service clicked on this page while logged into Facebook, it made the Facebook user automatically "like" several pages with no further interaction.
Source: http://www.networkworld.com/news/2010/051910-facebook-fixing-embarrassing-privacy.html?hpg1=bn

64. *May 18, IDG News Service* – (National) **FTC targets privacy concerns related to copy machines.** The U.S. Federal Trade Commission has begun contacting copy machine makers, resellers and office-supply stores about privacy concerns over the thousands of images that can potentially be stored on the machines' hard drives. The FTC chairman, in a letter to a U.S. Representative, said the agency has been working to alert copy-machine manufacturers and sellers of the privacy risks of the information that many copy machines store on their hard drives. The FTC is trying to "determine whether they are warning their customers about these risks ... and whether manufacturers and resellers are providing options for secure copying," the chairman wrote in a letter released May 18 by the Representative's office. CBS News, in a report that aired April 19, said that nearly every copy machine built since 2002 stores documents copied, scanned and e-mailed by the machines on their hard drives. The report found sensitive health and law-enforcement investigation information on copy machines ready to be resold. The Representative, in an April 29 letter to the FTC, called on the agency to investigate privacy concerns related to copy machines.
Source:

http://www.computerworld.com/s/article/9176928/FTC_targets_privacy_concerns_related_to_copy_machines

65. *May 18, Help Net Security* – (International) **Combat the malvertising threat.** Malicious advertising, also referred to as "malvertising," is a relatively new attack vector for cyber criminals that is quickly on the rise. With malvertising, fake malicious ads are delivered (often via advertising networks) to well-known Web sites as a way to reach millions of users at once on Web sites they normally trust. Unlike typical spam or virus attacks, which rely on victims to click on a link in an e-mail or accidentally download an infected program, malvertising attacks are presented on popular Web sites and can download malicious code directly onto a user's computer when the victim views the compromised ad. By infiltrating an entire ad network, the criminal gains access to a broad number of syndicated Web sites that can spread malicious code even further. Millions of users have been infected by malvertising threats recently, as evidenced by the high-profile attacks on The New York Times, Gizmodo, TechCrunch, WhitePages.com and other sites. Based on data generated from Dasient's telemetry system, there are approximately 1.3-million malicious ads viewed per day. Traditionally, many publishers and ad networks only respond to a bad ad when a user complains about the problem, and one complaint could mean thousands have been infected already by a malvertisement. To deal with the threat, publishers and ad networks have had to manually investigate reports of bad ads, which takes time and resources. Because attacks are sporadic, it makes the source of the bad ad very hard to pin down. To-date, publishers and ad networks have not had an automated solution to address the malvertising problem.
Source: http://www.net-security.org/secworld.php?id=9305

66. *May 17, Technology Review* – (International) **Commercial quantum cryptography system hacked.** When it comes to secure messaging, experts say nothing beats quantum cryptography, a method that offers perfect security. Messages sent in this way can never be cracked by an eavesdropper, no matter how powerful, according to experts. At least, that is the theory. On May 17, three researchers at the University of Toronto in Canada said they have broken a commercial quantum cryptography system made by the Geneva-based quantum technology startup ID Quantique, the first successful attack of its kind on a commercially available system. Any proof that quantum cryptography is perfect relies on assumptions that do not always hold true in the real world. Identify one of these weaknesses and a loophole is found that can be exploited to hack such a system. The new attack is based on assumptions made about the types of errors that creep in to quantum messages. However, it is impossible to get rid of errors entirely, so some errors must be tolerated. Various proofs show that if the quantum bit error rate is less than 20 percent, the message is secure. However, these proofs assume that the errors are the result of noise from the environment. The researcher say that one key assumption is that the sender can prepare the required quantum states without errors. She then sends these states to the receiver and together they use them to generate a secret key that can be used as a one-time pad to send a secure message. But in the real world, the sender always introduces some errors into the quantum states she prepares and it is this that the researcher have exploited to break

the system.
Source: http://www.technologyreview.com/blog/arxiv/25189/

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

67. *May 19, BBC* – (International) **Europe outlines plan to boost broadband by 2020.** Half of European households will have broadband speeds of 30Mbps (megabits per second) by 2020, the European Union has pledged. It also promised universal broadband coverage by 2013 while getting half of Europeans using public services and shopping online by 2015. It is part of the European Union's five-year plan for the digital economy. The raft of measures were announced by the newly-appointed digital affairs commissioner. The EU's digital agenda will see over 30 laws introduced over the next three years. Laying out her plans, the commissioner said that the EU invested 40 percent less in technology than the U.S. It meant that nearly a third of Europeans had never used the Internet and only 1 percent had access to fiber-based high-speed networks. In order to catch up, EU governments must double their annual spending on research and development to 11bn euros (Â£9.4bn) by 2020.
Source: http://news.bbc.co.uk/2/hi/technology/10128190.stm

68. *May 18, Government Technology* – (National) **FCC waivers and funding could fuel nationwide public safety network.** The FCC took a significant step toward building a nationwide public safety network last week by clearing the way for 21 cities, counties and states to begin building their own fourth-generation wireless networks. The commission gave conditional approval May 12 to waiver requests from New Jersey, Los Angeles County, Boston and 18 other entities to start creating 4G networks known as Long Term Evolution (LTE) networks. These networks could begin to form a nationwide interoperable wireless network that has been sought by public safety officials since September 11, 2001 terrorist attacks on the U.S. The FCC's National Broadband Plan calls for creating a nationwide public safety network within the 700 MHz D Block of radio spectrum formerly used by television broadcasters. In 2008, the commission attempted to auction the D Block spectrum to commercial telecom providers, with the winner required to build a nationwide network and share it with public safety agencies. But there were no takers, and a new D Block auction is not expected until 2011. The LTE networks approved last week will use 10 MHz of spectrum that public safety was granted in 1997. But the FCC required that the new networks be compatible with the proposed national D Block 700 MHz network.
Source: http://www.govtech.com/gt/articles/763523

[Return to top]

Commercial Facilities Sector

69. *May 19, WESH 2 Orlando* – (Florida) **Techs to test suspicious device found at Walmart.** Bomb-squad technicians will be testing a suspicious device that was found May 18 at a shopping center in St. Cloud, Florida, the discovery of which prompted police to evacuate a Wal-Mart and other stores. Authorities received two bomb threats May 18, the first of which was called into St. Cloud Hospital shortly after 6:15 a.m. St. Cloud police said a security guard received a call indicating a bomb was inside the hospital. Nothing was found in that investigation, and no evacuation took place. In the second incident, St. Cloud police received a call about a suspicious device at the Walmart at 4400 13th St. "(The) St. Cloud Police Department received a phone call at approximately 1:43 p.m. today (May 18) from the manager of St. Cloud's Walmart reporting that there was a bomb in the store and that it would go off in 30 minutes," according to a statement released by St. Cloud police. An evacuation of the Walmart and neighboring stores lasted about five hours, and a bomb-sniffing dog from Osceola County assessed the device. Police said they located a suspicious device outside the store, between the Walmart and the Bank of America at 4300 13th St., near a tree, and marked off the area. The Orange County Sheriff's Office Bomb Squad was called in to dismantle the device. Nothing was detonated. Investigators said they are not certain what the device was. Authorities have not identified any suspects or persons of interest. Investigators continue to interview witnesses and check surveillance video.
Source: http://www.wesh.com/news/23596519/detail.html

70. *May 19, The McDowell News* – (North Carolina) **Walmart evacuated; 12 sent to hospital.** A mixture of chemicals at Walmart in McDowell County, North Carolina Tuesday evening forced the evacuation of the store and sent a dozen people to the hospital. The Marion, North Carolina fire chief said an employee combined a couple of cleaners in the back of the store in preparation of scouring the bathrooms. He stated that he is not positive what chemicals were mixed, but he believes it was an absorbent substance used in RV tanks and Clorox. The employee was overcome by fumes, and the smell eventually got to others. The EMS director said 12 people were transported to McDowell Hospital, complaining of respiratory and eye irritations. Twelve more refused treatment or transport at the scene. The majority, if not all, of the patients were employees. The call came into the 911 center at 6:03 p.m. Members of the Marion Fire Department, McDowell County EMS, McDowell County Rescue Squad, Marion Police Department, and McDowell County Emergency Management responded to the scene and immediately evacuated the building. The fire chief stated that he got samples of the mixture, and that officials will continue to examine it. Walmart reopened shortly after 8 p.m.
Source: http://www2.wspa.com/news/2010/may/19/2/walmart-evacuated-12-sent-hospital-ar-178264/

71. *May 18, WCBS 2 New York* – (New Jersey) **N.J. landlord arrested in alleged homemade bomb case.** A New Jersey landlord remained under arrest May 18, accused

of trying to frame one of his tenants by blowing up the pizza shop in his own building, located at 451 Palisade Avenue in Jersey City. Investigators said the landlord led firefighters to the shop May 17 morning and even pointed out the crudely made device, a 2.5 gallon gas can wired to a light fixture that was rigged to go off when someone opened the pizzeria's front door. Neighbors were evacuated and the device was disabled. "It would have been a major explosion. Probably would have took that building and any building on either side of it," said a deputy chief of the JCPD. After searching the landlord's van, it didn't take detectives long to identify him as the suspect. Inside, police apparently found evidence that connected the landlord to the device inside the shop. No one was hurt.
Source: http://wcbstv.com/topstories/explosive.device.nj.2.1700081.html

72. *May 18, United Press International* – (California) **Nuclear terror drill held in Los Angeles.** The FBI Tuesday conducted the second day of what it says will be a three-day nuclear terrorism exercise in Los Angeles. The exercise that began Monday involves a team of state, local and national agencies dealing with an improvised nuclear bomb planted at the landmark Los Angeles Coliseum. The FBI said in a written statement the scenario involves finding not only the bomb, but also secondary devices in Los Angeles. Once located, the "bomb" will be disabled and hauled away to a safe location. A plot twist includes the detonation of another device in another part of the United States.
Source: http://www.upi.com/Top_News/US/2010/05/18/Nuclear-terror-drill-held-in-Los-Angeles/UPI-29401274226048/

[Return to top]

National Monuments and Icons Sector

73. *May 19, The Bay City Times* – (Michigan) **Grayling forest fire size now 7,500 acres, residents still can't return to homes.** A forest fire that started May 18 in Huron National Forest in Crawford County, Michigan has spread to about 7,500 acres and residents still cannot return to their homes. The fire started on Meridian Road in Grayling, Michigan and moved rapidly west southwest. The cause of the fire is still under investigation. Sixteen miles of trenches were dug overnight to keep the fire from continuing to spread. By 7 p.m. May 18, authorities reported that more than 5,000 acres had been affected. Preliminary reports are 10 structures have been engulfed by the fire. Road closures are still in place.
Source: http://www.mlive.com/news/bay-city/index.ssf/2010/05/grayling_forest_fire_size_now.html

74. *May 19, WFOR 4 Doral* – (Florida) **Coast Guard: Tar balls in Keys not from oil spill.** Dozens of tar balls found in Key West did not come from the Deepwater Horizon oil spill in the Gulf of Mexico. That information was released Wednesday morning from the U.S. Coast Guard after conducting lab tests on the tar balls discovered on beaches at Fort Zachary Taylor State Park, Smathers Beach in Key West, Big Pine Key, and Loggerhead Key in the Dry Tortugas National Park. The source of the tar balls

remains unknown at this time. Tar balls often wash up on the shores of Florida from cruise ships, oil tankers and other vessels which sometimes flush their almost-empty fuel tanks to clean them for another load. The tar-ball discovery put Florida's $60-billion tourism industry on its highest alert level since BP's Deepwater Horizon oil rig sank April 22, sending oil gushing into the Gulf of Mexico hundreds of miles from the Sunshine State. The public is reminded that tar balls are a hazardous material, which while not dangerous to most people can cause an allergic reaction and should only be retrieved by trained personnel. All beaches on the Florida Keys remain open.
Source: http://cbs4.com/local/Tar.tar.balls.2.1702654.html

[Return to top]

Dams Sector

75. *May 19, WVUE 8 New Orleans* – (Louisiana) **Work continues on the Great Wall of Orleans-St. Bernard.** Nearly two miles long and 26-feet high, the Lake Borne Storm Surge Barrier costs $1.3 billion, the single most expensive project in Louisiana history. "Everything you see there has been built since this time last year," said the resident engineer for the U.S. Army Corps of Engineers. The barrier is designed to plug the funnel, the infamous "v" shape in the levee, where the Mississippi River Gulf Outlet meets the Intracoastal Waterway. "What you have is massive water from all across the entire marsh against this wall," he said. "It is like a volume of water the size of Colorado coming to visit New Orleans and we are gonna try to keep that water out." The Corps, beaten and battered over the failures in Hurricane Katrina, is anxious to show off the results. The barrier's floodwall is made up of circular, reinforced, spun-cast piles driven more than 100-feet deep. Construction crews drove other piles at an angle to support the wall. A concrete cap, 12-feet wide, now makes it possible to walk, or drive, across the wall. The Corps boasts that the new "Risk Reduction" system begins downstream, with the MRGO closure structure, a rock dam across the waterway. Next, comes the surge barrier, which ties into a new, more robust "T" wall levee 14 feet higher than its predecessor. In turn, that 1,000-foot section of wall meets a 5-mile long levee on steroids, where the Corps has injected concrete 80 feet down to strengthen the levee. The method, known as "deep-soil mixing" allows the Corps to essentially construct a taller levee on top. Important gaps remain, at Bayou Bienvenue and the Intracoastal, where construction crews are building floodgates. The Corps, racing a deadline of June 1, 2011 to provide 100-year-storm protection, vows it will meet the goal even if some construction stretches into the later summer months.
Source: http://www.fox8live.com/news/local/story/The-Great-Wall-of-Orleans-St-Bernard/vlWosqe5a0uqbO6mTotPRw.cspx

76. *May 19, HNTB Corporation* – (National) **Americans too confident in flood, hurricane preparedness.** While a new America THINKS survey from HNTB Corporation shows six in ten (60 percent) Americans believe their area is prepared to deal with the potential damage from an extreme storm, hurricane or extensive flooding, events this spring have shown otherwise. "Recent flooding in Nashville put our flood management and levee systems to the test — and they failed," said the HNTB flood-

management practice leader. In 2009, the American Society of Civil Engineers gave the nation's levees a grade of D- in its Report Card for America's Infrastructure. More than half (55 percent) of Americans believe that if there is a major storm, hurricane or flooding event this year, their home or neighborhood will experience severe damage. With the threat of a busy Atlantic hurricane season, Southerners perceive themselves at greatest risk of a big storm or flood in the next five years (78 percent), while people in Western states perceive themselves at lowest risk (46 percent). "Additional education is needed to inform the public of the true threats in their region and what can be done to manage their flood risk," he said. Nearly every state has some level of storm-related flood risk. Flooding is the biggest natural threat to homes and properties nationwide, yet just 39 percent of Americans think so. According to ASCE, there is a 26 percent chance a 100-year flood event will occur during the life of a 30-year mortgage. When asked to estimate what percentage of levees in the United States are in disrepair, 42 percent of Americans simply said they did not know. The average response among the remaining 58 percent was that almost two-thirds (63 percent) of levees were in need of some kind of improvement.
Source: http://www.prnewswire.com/news-releases/americans-too-confident-in-flood-hurricane-preparedness-94251249.html

77. *May 18, WDEF News 12 and Associated Press* – (Tennessee) **TVA decides to store ash at Kingston spill site.** The Tennessee Valley Authority (TVA) in the next phase of its coal ash cleanup has decided to permanently store on site the ash that was not spilled in the river at its Kingston power plant west of Knoxville. That is the cheapest of several options TVA considered while receiving public comment. The on-site storage plan includes closing the pond contained behind an earthen dam that failed in December 2008. This second phase is expected to cost about $270 million and take about four years. TVA said in a statement Tuesday that the Environmental Protection Agency and the Tennessee Department of Environment and Conservation have approved the plan. The nation's largest public utility is finishing the first phase of the cleanup that has involved dredging ash from the Emory River.
Source:
http://wdef.com/news/tva_decides_to_store_ash_at_kingston_spill_site/05/2010

[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