Homeland Security

Daily Open Source Infrastructure Report for 7 September 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- The discovery of a suspicious package at Miami International Airport September 2, brought out a bomb squad and forced the evacuation and closing of four terminals for about 7 hours, CBS and the Associated Press reported. Tests eventually concluded the package was not hazardous. (See item **19**)
- According to CBS 13 Sacramento, Folsom State Prison in Folsom, California remains locked down and could stay that way for weeks while authorities investigate the circumstances surrounding an August 27 riot that left five inmates wounded from guards' bullets. (See item **43**)

Fast Jump Menu

PRODUCTION INDUSTRIES
- Energy
- Chemical
- Nuclear Reactors, Materials and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SUSTENANCE and HEALTH
- Agriculture and Food
- Water
- Public Health and Healthcare

SERVICE INDUSTRIES
- Banking and Finance
- Transportation
- Postal and Shipping
- Information Technology
- Communications
- Commercial Facilities

FEDERAL and STATE
- Government Facilities
- Emergency Services
- National Monuments and Icons

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. *September 3, Lacrosse Tribune* – (Wisconsin) **River weeds force power plant shutdown.** Dairyland Power Cooperative's Genoa, Wisconsin plant had to shut down for 5 days in August after weeds from the Mississippi River clogged its cooling system. The system's intake valves were completely plugged by vegetation, forcing the plant to

be taken off line from August 14-19, the Genoa plant site manager, said September 2. The plant was brought back online after Brennan Marine cleared vegetation from the intake valve area. Thick vegetation can affect the plant in the fall when it dies off and flows downstream, but rarely in August, he said. The last time the plant had to be taken offline was October 26, 2008, again due to weeds and other growth.
Source: http://lacrossetribune.com/news/local/article_f9e9144c-b70f-11df-8d28-001cc4c03286.html

2. *September 2, Homeland Security Today* – (National) **Report: Nation's pipeline security uncertain.** As part of DHS's mission to protect the nation's critical energy sector pipeline systems that are prime targets of terrorists such as Al Qaeda and its associated movements, the Transportation Security Administration's Pipeline Security Division (PSD) has been tasked to assess the risk and prioritize efforts to help strengthen pipeline security across the United States. But while PSA has identified the 100 most critical pipeline systems and developed pipeline risk assessment model based on threat, vulnerability and consequence, it nevertheless "could improve the model's consequence component and better prioritize its [security risk assessment] efforts," the Government Accountability Office (GAO) concluded in the report of its recent audit of PSD's pipeline infrastructure security efforts. In "Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes," GAO said that "the consequence component takes into account the economic impact of a possible pipeline attack, but not other possible impacts such as public health and safety, as called for in [DHS's] risk management guidance. PSD plans to improve its model by adding more vulnerability and consequence data, but has no time frames for doing so." GAO reviewed PSD's risk assessment process and performance measures and observed 14 PSD reviews and inspections. The government watchdog agency recommended that TSA, among other things, establish time frames for improving risk model data, document its method for scheduling reviews, and develop a plan for transmitting recommendations to operators.
Source: http://www.hstoday.us/content/view/14575/149/

3. *September 2, KTRK 13 Houston* – (Texas) **Residents evacuated after big rig overturns.** A tanker truck accident had most of FM 1462 in Rosharon, Texas, closed down for hours September 2. The road was blocked off from state Highway 288 to County Road 121 for hours. People who live in the area were evacuated. The tanker truck appeared to have been pulling into a Conoco gas station when it tipped over. A second tanker has been brought in to offload the gas in the tanker. The First Baptist Church in Angleton set up a shelter for people who needed a place to go during the evacuation.
Source: http://abclocal.go.com/ktrk/story?section=news/local&id=7647000

[Return to top]

Chemical Industry Sector

4. *September 3, Huntington Herald-Dispatch* – (West Virginia) **Study of MIC storage at W.Va. plant under way.** The National Academy of Sciences is studying how to best reduce or eliminate the storage of a toxic chemical at Bayer CropScience's plant in Institute, West Virginia. The U.S. Chemical Safety Board said September 2 that the $575,000 study will look at the storage of methyl isocyanate, or MIC. The board chairman said he hopes the study will be a model for the chemical industry to assess and reduce toxic hazards. Bayer has said it plans to cut storage of MIC at the plant by 80 percent and build an underground storage tank to hold the chemical. An above-ground storage tank was near the site of a blast that killed two employees in 2008. No MIC was released, but the explosion raised concerns about what could happen if a future mishap damaged the tank.
Source: http://www.herald-dispatch.com/business/x1431852405/Study-of-MIC-storage-at-W-Va-plant-under-way

5. *September 3, Columbus Republic* – (Indiana) **I-74 closed near Indiana-Ohio state line after tanker crashes, spills chemical.** All lanes of Interstate 74 in St. Leon, Indiana were shut down after a semi tanker hauling a hazardous chemical crashed and overturned. State police said the tanker leaked around 10 gallons of the chemical phtalic anhydride molton after the crash early September 3 about 10 miles west of the Indiana-Ohio state line. The truck driver told troopers the tanker's 4,000 gallons of liquid shifted on uneven pavement in a construction zone and the truck hit the concrete barrier before overturning. Police said the trucker was taken to a Cincinnati, Ohio hospital with a head injury. Police said the spilled chemical was contained and that crews were waiting to clean it up. An official said the crash was in a rural area and that he knew of no evacuations that were needed.
Source:
http://www.therepublic.com/view/story/c9a32e49e2d443a5b5663097369ff0ec/IN--I-74_Tanker_Crash/

6. *September 2, U.S. Environmental Protection Agency* – (Missouri; Kansas; Illinois) **Kahoka, Mo., landowners and two businesses ordered to halt hazardous waste pollution at chemical processing site.** The Environmental Protection Agency (EPA) has ordered the owners of a Clark County, Missouri, property, along with an Illinois minerals brokerage firm, and a Missouri company that processes materials at the location, to immediately halt the handling and processing of hazardous materials that have contaminated the property and an adjacent stream. TNT General Contracting, Inc., of Kahoka, Missouri; Webb Minerals, LLC, of Quincy, Illinois; and the Carl and Carol Trump Trust, of Kahoka are the respondents of a unilateral administrative order issued September 2 by EPA Region 7 in Kansas City, Kansas. The order directs the respondents to take a series of actions, including the development of a plan to clean up the property and any surrounding areas that may be polluted. The EPA indicated that the Missouri Department of Natural Resources sampled water on the site and found many chemicals had been discharged into the Weaver Branch tributary of the Mississippi River, including boron, arsenic, copper, ammonia, zinc, chromium, cobalt, manganese, nickel, selenium, aluminum, barium, cadmium and 2-Butanone. MDNR soil samples turned up zinc, barium, mercury, nickel, 2-Butanone, tetrahydrofuran,

toluene, arsenic, cadmium, chromium and lead. EPA's administrative order becomes effective within 5 days of the filing. The order further outlines a series of deadlines and schedules for initiation or completion of its required activities.
Source: http://yosemite.epa.gov/opa/admpress.nsf/0/914a4c3becb49e4e8525779200784ab5?OpenDocument

7. *September 2, Associated Press* – (International) **Thieves steal 2 tons of explosives in Brazil.** Authorities said armed men stole a truck with more than 2 tons of explosives from a chemical company in Brazil. Police said five men in two vehicles blocked the truck and held the driver hostage for several hours so they could gain time to flee. The truck's tracking system was turned off immediately after it was stolen. The army said in a statement September 2 that it will investigate whether the unnamed company had enough security measures. Police said they do not yet have enough information to link the robbery to terrorist groups or organized crime.
Source: http://www.msnbc.msn.com/id/38979117/ns/world_news-americas/

For more stories, see items **8** and **31**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *September 3, KGO 7 San Francisco* – (California) **Depleted uranium found at murder suspect's home.** In San Francisco, California, police are still sorting through the grisly details of a killing spree. The suspect was shot to death August 31 after a high-speed chase, and authorities found several bodies in his Vallejo home as well as chemicals, including depleted uranium. In the complicated case, it turns out a husband of one of the murder victim's was living in the murder suspect's home along with dead bodies. The husband, a chemist, is now in jail facing charges of possessing a collection of highly explosive materials authorities confiscated from the home. For the past 16 years, the husband worked as a chemical engineer at Goodrich in Fairfield, a company that makes propulsion mechanisms for all types of aircraft. Police still will not specify what chemicals were found at the chemist's home and storage unit, but the materials also included the military explosive C4, dynamite. The Bureau of Alcohol, Tobacco, Firearms and Explosives found a container labeled "depleted uranium." They are not sure what the items are until they are analyzed, said a lieutenant with the Vallejo Police Department.
Source: http://abclocal.go.com/kgo/story?section=news/local/east_bay&id=7646390

9. *September 3, Brattleboro Reformer* – (Vermont) **Yankee's new wells delayed.** The drilling of five new groundwater monitoring wells at Vermont Yankee nuclear power plant in Vernon, Vermont, has been delayed awaiting the completion of an engineering assessment. "We don't dig any holes at the plant without one," said Yankee's director of communications, adding the drilling has been delayed by 15 days. "We do a detailed review before we start doing any work on site." The new wells are to be located next to

buried underground pipes that run from the Advanced Off-Gas Building to the plant stack, according to information posted on the Vermont Department of Health's Web site. In January, Entergy, which owns and operates Yankee, told the Vermont health department that tritiated water had been discovered in a groundwater monitoring well on-site. The leak was traced to a pipe tunnel adjacent to the off-gas building. The leak was due to a clogged sump pump. After the sump was cleared in February, the leak was stopped. As of August 26, approximately 245,000 gallons of tritium-contaminated groundwater has been pumped out from the site from three extraction wells. Entergy has set a goal of removing 300,000 gallons of contaminated water to help remediate soils.
Source: http://www.reformer.com/localnews/ci_15979262

10. *September 3, Nuclear Street* – (Mississippi) **Grand Gulf to be the Largest Single Nuclear Plant in the U.S., if approved.** According to ClarionLedger.com, Entergy Mississippi this month will present its plans for a $510 million expansion of the Grand Gulf nuclear plant near Port Gibson to federal regulators. If approved, Grand Gulf would make it the largest single-reactor nuclear plant in the nation. With approval from the Nuclear Regulatory Commission, the utility would increase the plant's output from 1,265 megawatts to 1,443 — a 13 percent increase, Entergy officials said. After the upgrade, Grand Gulf will be able to produce enough electricity to power an additional 53,000 homes for the life of the plant. The average home uses about 1,000 Kw-h per month, a company spokeswoman said. The upgrade is scheduled for February 2012 during regular maintenance outages, pending federal approval. Entergy expects it will take at least a few weeks, but has no definitive timetable for the expansion. The Mississippi Public Service Commission already has backed the effort, but federal approval is needed before work can start.
Source: http://nuclearstreet.com/blogs/nuclear_power_news/archive/2010/09/03/Grand-Gulf-to-be-the-Largest-Single-Nuclear-Plant-in-the-U.S_2E002C00_-if-approved.aspx

11. *September 2, Georgia Public Broadcasting* – (Georgia) **SRS spill prompts safety review.** Workers moving barrels of radioactive waste at the Savannah River Site near Augusta, Georgia noticed one of the containers leaking about 13 gallons of liquid plutonium. The area was immediately evacuated. But, according to a report released last week, it was more than 24 hours before cleanup started. The report from the Defense Nuclear Facilities Safety Board said the contamination was so severe that cleanup crews had to leave because their safety equipment was not adequate. A spokesperson for the site's operator Savannah River Nuclear Solutions (SRNS) said it is common to re-examine safety procedures after such an event. According to SRNS no one was hurt and the area has been contained.
Source: http://www.gpb.org/news/2010/09/02/srs-spill-prompts-safety-review

12. *September 2, AZoM News* – (Tennessee) **More nuclear materials removed from Y-12 National Security Complex.** The 613,642-square-foot Alpha 5 Building (also known as 9201-5) and the 7,700-square-foot 9720-38 Y-12 National Security Complex storage areas in Oak Ridge, Tennessee no longer carry nuclear designations, resulting in significant cost savings for operations. Shedding the nuclear facility status at Alpha 5

equals a savings of $220,000 annually in surveillance and maintenance expenditures alone. Add in the savings associated with utilities and environmental costs, and the benefit to taxpayers grows. "This is an important milestone as we continue to transform NNSA's Cold War-era nuclear weapons complex into a 21st century nuclear security enterprise," said the NNSA deputy administrator for defense programs. Built in 1945 to house the calutrons that enriched uranium for the Manhattan Project, Alpha 5 played a central role in nuclear component production through the Cold War. Building 9720-38 was a classified storage area. Also, last year, the 313,771-square-foot Beta 4 building (also known as 9204-4) received its non-nuclear designation.
Source: http://www.azom.com/news.asp?NewsID=24016

[Return to top]

Critical Manufacturing Sector

13. *September 3, CNN* – (National) **Kia recalling fire-prone cars.** Hyundai-Kia Motors is recalling more than 35,000 cars with fire-prone electrical wiring systems, said the National Highway Traffic Safety Administration. The government agency said September 3 that the recall extends to some 2010-2011 Kia Soul and Kia Sorento models manufactured between Sept. 7 2009 and July 30, 2010. "When lights are illuminated under certain conditions, an electrical short may occur that can result in a fire," said the recall notice. The South Korean automaker said the faulty wiring is from the interior lighting in front and rear door trim panels, which are the plastic moldings on the inside of the car.
Source:
http://money.cnn.com/2010/09/03/autos/hyundai_kia_recall/index.htm?cnn=yes&hpt=T2

14. *September 3, Occupational Health & Safety* – (International) **Brass foundry cited for 'deliberate' lead-exposure hazards.** The Occupational Safety and Health Administration (OSHA) has issued citations to Kief Industries Inc., doing business as Excelsior Brass Works. The citations allege the company knowingly exposed workers to lead hazards and violated federal workplace safety and health standards at its Blandon, Pennsylvania facility, which manufactures brass and bronze castings. Proposed penalties total $550,400. "The employer deliberately refused to protect workers from overexposure to lead and other workplace hazards. Even though company management knew of the OSHA requirements and the workers' lead exposures, it failed to provide medical surveillance to monitor worker health and to train its workers about lead-exposure risks," said OSHA's Assistant Secretary of Labor.
Source: http://ohsonline.com/articles/2010/09/03/brass-foundry-cited-for-lead-overexposure.aspx?admgarea=news

15. *September 1, Houston Business Journal* – (Texas) **Goodman Manufacturing faces OSHA fine.** Goodman Manufacturing Co. LP may have to pay more than $1.2 million in fines for allegedly failing to record or improperly recording injuries at one of its Houston, Texas facilities. The Occupational Safety and Health Administration (OSHA)

said September 1 it had issued 83 citations against the company related to its air conditioning cooling facility in Houston. Goodman manufactures residential and light commercial air conditioning, heating and indoor air quality products. The workplace safety organization said it found that Goodman failed to properly record the nature and duration of 72 percent of employee injuries and illnesses from January 2008 to March 2010 on its log. In a statement, Goodman said the alleged violation involved clerical errors. "Goodman strongly disagrees with OSHA's position regarding these paperwork issues and intends to vigorously contest this citation," the statement said. The company has 15 business days to comply or contest the citations, according to OSHA.
Source: http://houston.bizjournals.com/houston/stories/2010/08/30/daily29.html

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

16. *September 3, SC Magazine* – (International) **Cyber criminals seek 'full' sets of credentials that trade for only a few pounds.** Malicious software kits are available for under Â£2,000 on the Internet, while online bank logins trade for just Â£32. A report by RSA revealed that Zeus Trojan kits are now on sale for Â£1,944 in some cases. Basic kits for the SpyEye Trojan, what the RSA FraudAction Intelligence Team called "2010's biggest Trojan innovation" and "the only commercially available banking Trojan able to challenge Zeus' market-share," are available for under Â£700. A Firefox injection tool is available for anywhere between $1,000 and $2,000. RSA's online fraud report for August said: "If you were to take a glimpse into the fraud black market, you would see that not only do cyber criminals trade stolen data, but they also offer a multitude of tools and services for sale that enable others to harvest this information and/or monetize it. Examples of some criminal 'product' offerings would include fraudster call center services that 'outsource' fraudulent phone calls made to banks or merchants; information services that provide a rich set of personal and financial data on potential victims; phishing kits that target different banks: Trojan infection kits; and credit card checking services, just to name a few." It also reported on how seasoned fraudsters are opting for the purchase of "Fulls," which comprise the genuine cardholder's information including online banking account (via username and password combination), billing address, credit card number, CVV2 code, expiration date, mother's maiden name, date of birth and Social Security number.
Source: http://www.scmagazineuk.com/cyber-criminals-seek-full-sets-of-credentials-that-trade-for-only-a-few-pounds/article/178181/

17. *September 3, SC Magazine UK* – (International) **Heartland pays $5 million over 2008 intrusion to credit card provider.** Heartland Payment Systems must pay $5 million to

a financial services customer over the 2008 data breach. In a statement that describes the payment to Discover as an "intrusion settlement," Heartland confirmed it will pay Discover $5 million to resolve "all issues related to the 2008 intrusion." Heartland's chairman and chief executive officer, said: "We are pleased to have reached an equitable settlement with Discover." The payments processor had already paid American Express $3.6 million over the same breach, while Visa agreed to cap its compensation demands to $59.2 million, according to Australia's IT News. The Heartland incident was initially believed to have affected over 100 million cards, after intruders broke into the systems and planted malicious software to steal card data carried on the company's networks. One estimate claims that as many as 130 million cards were affected. The incident led to a Colorado bank blocking all point of sale purchases on issued debit cards, while Heartland's CEO called for better industry collaboration and information sharing.
Source: http://www.scmagazineuk.com/heartland-pays-5-million-over-2008-intrusion-to-credit-card-provider/article/178180/

18. *September 1, Infosecurity* – (International) **New Zeus campaign uses FedEx notice scam.** Security firm McAfee has alerted the online community to a new Zeus botnet attack using bogus FedEx notification e-mails. McAfee malware research scientist made note of the new Zeus push August 31 in a McAfee Labs blog posting. The scientist said the new spam campaign is linked to the Asprox botnet, which is spreading e-mails that use FedEx branding. The research scientist said these fake FedEx e-mails contain attachments that are really executables, with file names starting in FedExDoc or FedExInvoice. "Those attachments are recognized as the Bredolab Trojan," wrote one Malware research scientist, "which will download the Zeus component." Zeus is the notorious Trojan delivered via e-mail files with .exe attachments, and is designed to make off with personal and banking information. Malware research scientist also added that several large U.S. banks are among targets of the fake FedEx e-mails –- including Citibank, Comerica, USBank and Wells Fargo –- in addition to several other banks in Europe, the Middle East, Asia, and South America.
Source: http://www.infosecurity-us.com/view/12149/new-zeus-campaign-uses-fedex-notice-scam/

[Return to top]

Transportation Sector

19. *September 3, CBS & Associated Press* – (National) **Scientist in Miami Airport scare has rap sheet.** The discovery of a suspicious package at Miami International Airport September 2, brought out a bomb squad and forced the evacuation and closing of four terminals for about 7 hours. Tests eventually showed that the passenger, the suspicious metal canister in his luggage, and his other belonging did not contain any hazardous biological material or explosives. But a senior law enforcement official indicated that the passenger who was detained in the incident, was a scientist who had once been charged with illegally transporting bubonic plague. He was acquitted of the charges of transporting the potentially deadly germ in 2003. The scientist cooperated fully

September 2 after he arrived on a flight from the Middle East, said the official, who requested anonymity because he wasn't authorized to release the information. Most of Miami International was shut down September 2 after a Transportation Security Administration officer found what appeared to be a pipe bomb in the scientist's luggage.
Source: http://www.cbsnews.com/stories/2010/09/03/national/main6833392.shtml

20. *September 2, KUSA 9 Denver* – (Colorado) **Gun in purse at DIA gets father, daughter in trouble.** A man and his daughter both face charges after she had a gun in her purse when she tried to get through security at Denver International Airport (DIA) in Colorado. Investigators said a 44-year-old man gave his daughter, a juvenile, a .22 caliber handgun for self protection. She forgot the loaded gun was in her purse and the Transportation Security Administration found it when she went through security at DIA. The two, who live in Aurora, were going to take a Delta Airlines flight to Salt Lake City, Utah. The handgun had four live rounds inside, according to police. He is charged with unlawfully providing or permitting a juvenile to possess a handgun and contributing to the delinquency of a minor. His daughter was charged with possession of a handgun by a juvenile. The man was released on $10,000 bond and will appear in court September 17. He was previously charged with having a handgun at DIA in 2005, but he was acquitted in 2007.
Source: http://www.9news.com/news/article.aspx?storyid=150973&catid=339

21. *September 2, Wall Street Journal* – (New York) **LIRR to suspend service on two branches as Hurricane Earl nears.** With Hurricane Earl expected to bring tropical-storm conditions to the New York metropolitan area, the Long Island Rail Road moved to suspend service on its two East End branches starting September 3. The service suspension means that thousands of New Yorkers who ride the Montauk and Ronkonkoma Branch trains to the Hamptons and the North Fork had to find other ways to the beach for Labor Day weekend. Service was suspended east of Speonk on the Montauk Branch and east of Ronkonkoma on the Ronkonkoma Branch. LIRR officials were worried that high winds from Hurricane Earl would snap crossing gates, down trees and knock out power lines. "We don't want a train with a thousand people on it that can't proceed because of a broken gate or a broken wire or down trees," said an LIRR spokesman.
Source: http://blogs.wsj.com/metropolis/2010/09/02/lirr-to-suspend-service-on-two-branches-as-hurricane-earl-nears/

22. *September 2, Aviation Week* – (Virginia) **TSA mulls changes for DCA access.** The Transportation Security Administration (TSA) is looking at short-term initiatives to increase access to Ronald Reagan Washington National Airport (DCA), but continues to strive for long-term changes to some of the more prohibitive requirements for use of the airport. The manager of TSA's General Aviation branch said he has an "open goal of increasing flights into DCA" and called for a summit involving operators and Washington-based association representatives to discuss possible changes that would encourage more business aircraft operations. The discussions centered on issues with the DCA Access Standard Security Program (DASSP), and TSA is considering ways to

improve processing, "which is one of the inhibitors for DCA use," according to the manager. Other actions include increasing the number of gateway airports, which are airports approved for direct flights into DCA. TSA has expanded its list of gateways to more than 30 airports, the most recent of which includes Nashville.
Source:
http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=busav&id=news/awx/2010/08/30/awx_08_30_2010_p0-251055.xml&headline=TSA Mulls Changes For DCA Access

23. *September 2, Arlington Heights Daily Herald* – (Illinois) **Plane returns to O'Hare safely after lightning strike.** Passengers aboard an American Airlines jet bound for Reno, Nevado had a short but eventful flight after lightning struck their 737 September 2. The plane left Chicago O'Hare International Airport at 10:16 a.m. carrying 160 passengers and five crew members, an American Airlines spokeswoman said. After lightning hit the front windshield area, the pilots declared an emergency and the plane returned to O'Hare without incident. The jet was taken out of service and mechanics are looking at the air-conditioning system for damage. Lightning strikes are fairly uncommon but they do occur and airplanes are designed and tested for that eventuality.
Source: http://www.dailyherald.com/story/?id=405360&src=1

24. *September 2, Cincinnati Courier-Journal* – (Kentucky; Alabama) **Trucking firm ordered to close after Int. 65 accident that killed 11.** The Alabama trucking company whose driver slammed into a van on Interstate 65 near Munfordville, Kentucky in March 2010, killing 10 people and himself, has been ordered to cease operations after a federal agency found it had committed serious safety violations. The Federal Motor Carrier Safety Administration ordered Hester Inc. of Fayette, Alabama off the road in June when it failed to correct "critical" violations, which included allowing operators to drive longer than allowed by law. Hester was fined $13,950 for the violations, but defaulted on the payments. The order to cease operations was effective June 5 but not released until September 1. The order to cease operations said Hester cannot return to business until it is deemed "fit" by the federal agency and its registration is reinstated. A Kentucky State Police report on the March 26 fatal accident found that a truck driver was distracted and did not have his tractor-trailer under control when it crossed the median and rammed a van carrying a Mennonite family and friends traveling to an Iowa wedding. The report, issued in May, said the driver was talking on a cell phone and may have been speeding.
Source: http://news.cincinnati.com/article/20100902/NEWS0108/309020022/Feds-close-trucking-firm-after-crash

25. *September 2, Ventura County Star* – (California) **4 arrested in train trespassing sweep.** Four people were arrested September 2 on suspicion of trespassing on Union Pacific railroad property in southern California as local authorities looked for trespassers on private railroad property. The operation, which stretched from Camarillo to Montalvo, involved the Oxnard Police Department, the Ventura County Sheriff's Department, the Los Angles County Sheriff's Department, DHS, and agents from the Union Pacific Police Department. Agents and police also were looking for pedestrians,

motorists and bicyclists who failed to yield the right of way or obey train crossing signs and warnings at train track crossings. Officers said they witnessed 60 different violations. California ranked second in the nation in 2009 for collisions at train track crossings, with 121 accidents. Of these, 91 resulted in death. Moreover, 61 of these collisions were fatal trespasses and 42 were trespasses with injuries.
Source: http://www.vcstar.com/news/2010/sep/02/4-arrested-in-train-trespassing-sweep/

For more stories, see items **2**, **3**, and **5**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

26. *September 2, WTOV 9 Steubenville* – (West Virginia) **Grocery store evacuated after freon leak.** A refrigerator malfunction is to blame for a Freon leak September 1 that caused Weirton Shop N' Save, a Hancock County, West Virginia, grocery store to be evacuated. The store manager on duty at the time said no one was seriously injured, but everyone inside the store was forced to leave. About seven workers were examined by emergency crews outside of the store, and no one was transported to the hospital. The manager said repair workers fixed the leak and the store is open for business.
Source: http://www.wtov9.com/news/24854664/detail.html

27. *September 2, NaturalNews* – (Michigan) **Antibiotic tainted beef illegally sold for human consumption.** Scenic View Dairy of Hamilton, Michigan is currently the subject of a complaint filed by the U.S. Department of Justice (DOJ) on behalf of the Food and Drug Administration (FDA) for selling beef that tested positive for illegal levels of neomycin, penicillin and sulfadimethoxine. The FDA is seeking a permanent injunction against the dairy for ignoring multiple warnings about the tainted meat. According to reports, the FDA has warned Scenic View Dairy at least eight times since 2001 about unsafe levels of antibiotics in its beef, and the USDA has sent more than 11 letters concerning the issuel. But the defendants have ignored all such warnings given between 2002 and 2010, and have continued to sell the beef. FDA regulations specify that in order to sell meat for human consumption, the animals must be off antibiotics and other drugs for a certain period of time so the substances clear from their systems. But Scenic View Dairy's three farms have allegedly been selling the meat long before the proper time.
Source: http://www.naturalnews.com/029644_beef_antibiotics.html

28. *September 2, Food Product Design* – (California) **Shredded pork recalled in California.** Trinh Co., based in San Jose, California, is recalling approximately 2,070 pounds of cooked shredded pork skin products because they were produced without a federal inspection, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced September 1. The recall involves 8-ounce, 10-ounce and 5-pound clear plastic bags of "Trinh Co. Bi Tuoi Cooked Shredded Pork Skin, Thuong Hang Bi Tuoi V.N. Hop Ve Sinh." The recalled products were distributed to retail establishments in California. Each bag bears the establishment number "6488" inside the USDA mark of inspection.
Source: http://www.foodproductdesign.com/news/2010/09/shredded-pork-recalled-in-california.aspx

[Return to top]

Water Sector

29. *September 3, Sioux Falls Argus Leader* – (South Dakota) **Explosion hurts two workers.** Two Sioux Falls, South Dakota employees were injured August 30 when hot water erupted from a malfunctioning bypass pump near the site of the sewer pipe repair at Main Avenue and Walnut Street, and one is still in the hospital with burns over 30 percent of his body. The employees were attempting to repair the pump and were severely burned, said the city's risk manager. The men worked for the Water Reclamation Division. They were both transferred to a hospital in Sioux Falls where one was treated and released. The other was airlifted to a Twin Cities hospital. Two days later, it was reported the man was stable and comfortable.
Source: http://www.argusleader.com/article/20100903/NEWS/100903001/1001/news

30. *September 2, Des Moines Register* – (Iowa) **Monticello power outage sends sewage into Iowa river.** A power outage September 1 caused a sewage bypass in Monticello, Iowa, that sent 75,000 to 100,000 gallons of untreated sewage into the Maquoketa River. An alarm apparently malfunctioned and an emergency generator was out of service for repairs. The bypass ended when power was restored at 7 a.m. The Iowa Department of Natural Resources warned residents to stay out of the river in that area for 48 hours. Biologists warned that harmful organisms still may be present after that because the city's disinfection unit was damaged in the July flood. The state has ordered the city to use temporary disinfection equipment.
Source: http://blogs.desmoinesregister.com/dmr/index.php/2010/09/02/monticello-power-outage-sends-sewage-into-iowa-river/

31. *September 2, Lahontan Valley News* – (Nevada) **Third acid spill occurs at water treatment plant.** On September 1, the third hydrochloric acid spill in less than 2 weeks occurred at the water treatment facility in Fallon, Nevada. "It's just a very unfortunate series of events," said a city engineer, "We are definitely making sure we keep everyone safety-concerned." Water treatment operations were not interrupted. The third spill came after a 10,000-gallon acid spill during a delivery August 23, and a second spill of about 250 gallons August 24 when a gasket on a 330-gallon chemical tote came

loose. On each occasion. mitigation efforts built into the facility operated effectively and no one was injured. "The spills have all been properly contained," he said. "They've all been properly mitigated. It's just been a terrible series of bad luck that's led to this." He said at about 1:30 p.m. September 1, about 330 gallons of hydrochloric acid spilled outside near the acid-containment building after a portable tote fell off the back of a flatbed truck and cracked open. "It didn't go anywhere except for dirt and gravel," said a city spokeswoman. Since the clean-up contractor Clean Harbors Environmental was already on site working on the previous spill, they were able to mitigate and clean the new spill right away.
Source:
http://www.lahontanvalleynews.com/article/20100902/NEWS/100909966/1055&ParentProfile=1045

32. *September 2, U.S. Environmental Protection Agency* – (Missouri) **Orders issued to Missouri Department of Transportation for construction stormwater violations in Camden, Wayne Counties.** Environmental Protection Agency (EPA) Region 7 has issued a pair of administrative orders to the Missouri Department of Transportation (MoDOT), citing multiple violations of stormwater permits that were issued for state construction projects along U.S. Highway 54 Expressway in Camden County, and U.S. Highway 67 in Wayne County. EPA's orders, filed September 2 in Kansas City, Kansas, direct MoDOT to comply immediately with the terms of the respective permits for the two highway construction projects, which were issued to MoDOT by the Missouri Department of Natural Resources (MDNR) under the authority of the federal Clean Water Act.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/89D2CF326C44E45F852577920079BBE4

For more stories, see items **6**, **9**, and **58**

[Return to top]

Public Health and Healthcare Sector

33. *September 3, Associated Press* – (Oklahoma) **Ex-director of Tulsa's Reproductive Services charged with making false report about bomb scare.** According to court records, the former executive director of a Tulsa, Oklahoma clinic where abortions are performed has been accused of making a false report about a bomb scare at the clinic last month. Court documents show that the 63-year-old was charged the week of August 30 with providing false and misleading information about an alleged bomb. Her attorney declined to comment but said the lady is no longer employed at the clinic. Police were called to Reproductive Services August 13 after an employee reported a suspicious box in a trash can. A bomb technician determined it was not an explosive. The clinic was attacked three times in 1997: the building was firebombed with Molotov cocktails, damaged with pipe bombs and hit by gunshots. A teenager was placed on juvenile probation in connection with those crimes.
Source: http://www.kfor.com/news/sns-ap-ok--bombscare-clinic,0,5790229.story

34. *September 3, WRTV 6 Indianapolis* – (Indiana) **Human West Nile cases confirmed in Indiana.** The Indiana State Department of Health said September 3 that the first two confirmed cases of West Nile virus of the season were confirmed this week. One of the cases is in Marion County, and the other is in Allen County. The public relations coordinator of the Marion County Health Department (MCHD), said the department has been performing tests on mosquitoes in the county for 6 months. Central Indiana usually records human cases from late August through the end of the mosquito season, which generally happens at the first hard frost. "While not surprising, these human cases serve to remind all of us that mosquitoes with the West Nile virus are active and we must remain vigilant in protecting ourselves," said MCHD's director. Five people have died from West Nile virus in Marion County since 2002, with 52 human cases recorded.
Source: http://www.theindychannel.com/health/24869530/detail.html

35. *September 2, TMCnet* – (National) **SmartMetric's biometric card to provide personal medical records.** SmartMetric said that its fingerprint activated Biometric Data Card can be now used to provide the highest level of both security and portability for a person's medical history and full medical records. The SmartMetric Data Card can store Gigabytes of medical information including full EKGs, complete CT and MRI digital images, and similar data making up an individual person's complete medical records. Storage of digital images, in particular, requires significant digital storage capacities. Unlike other systems that are severely limited in the amount of digital data that can be held in a portable solution, The SmartMetric solution provides security for the patients information in that it can only be accessed after the patient touches the surface sensor on the Health Card triggering the Card to scan the persons fingerprint and matching it with their fingerprint pre-stored inside the card. Only after a finger print verification internally in the card is the data able to be accessed or viewed by a doctor, hospital or EMT's computer.
Source: http://www.tmcnet.com/usubmit/2010/09/02/4987396.htm

[Return to top]

Government Facilities Sector

36. *September 3, U.S. Army News Service* – (International) **Typhoon Kompasu strikes U.S. military garrisons in Korea.** Military garrisons in Korea were ready for Typhoon Kompasu, a Category 1 tropical cyclone that hit the peninsula early September 2 with 65-mph sustained winds. There have been no reported injuries of U. S. Army personnel, but the storm caused moderate, widespread damage. Damage assessment at Yongsan is still ongoing — multiple buildings and vehicles are still covered in trees and debris. Power has been restored in most areas, but efforts are still being made to return electricity to remaining areas. Although there were no power outages at USAG Humphreys, more than 200 trees were toppled and one aircraft hangar lost a portion of its roof. Other structures, such as warehouses and another hangar took minimal wind damage. Humphrey's public affairs officer said efforts were being made to salvage approximately 50 of the trees that were blown down. Osan Air Base, only a few miles

from Humphreys, also received minimal damage and brief power outages. USAG Red Cloud and Casey received no structural damage and only brief power outages despite the loss of about 100 trees. In the southern part of the peninsula, USAG Daegu was unaffected.
Source: http://www.army.mil/-news/2010/09/03/44683-typhoon-kompasu-strikes-us-military-garrisons-in-korea/

37. *September 2, KOB 4 Albuquerque* – (New Mexico) **Explosive device forces evacuation of nearby Los Lunas school.** Los Lunas Middle School in Albuquerque, New Mexico was evacuated September 2 as Los Lunas police investigated what they are calling an improvised explosive device. One firefighter described the device as a weird looking device containing a mysterious powder that looked like it could be potentially explosive. The device was moved by the Albuquerque Police Department bomb squad to a secure location.
Source: http://www.kob.com/article/stories/S1726624.shtml?cat=504

38. *September 2, Computerworld* – (Texas) **Texas county scrambles to replace e-voting machines destroyed in fire.** Officials in Harris County, Texas, are scrambling to find replacement e-voting machines for this year's gubernatorial elections after a massive fire last week destroyed all 10,000 machines originally scheduled for use in the polls. The pre-dawn fire, the cause of which still remains a mystery, destroyed a 28,000-square-foot warehouse in which the machines were stored, and caused close to $40 million in damages, according to a report in the Houston Chronicle. A county clerk told the Chronicle $30 million of the loss was tied to the voting equipment while the remainder stemmed from damages to the building. The e-voting machines were slated for use in 736 polling sites for the November 2 elections and for early voting, which runs Oct. 18-29. Harris County encompasses the city of Houston and bills itself as the largest county in the United States as well as the largest one to adopt e-voting technologies. The county has been using e-voting machines since 2001.
Source:
http://www.computerworld.com/s/article/9183463/Texas_county_scrambles_to_replace_e_voting_machines_destroyed_in_fire

39. *September 2, Los Angeles Times* – (California) **Live grenade forces evacuation of Glendale Community College campus, nearby homes.** A live Vietnam-era grenade was detonated September 2 at a Glendale Community College satellite campus in Glendale, California, according to the Los Angeles County Sheriff's Department. Investigators said the device was unearthed by construction crews at the Garfield Avenue campus. The discovery prompted the evacuation of the entire campus and several nearby residential buildings. About 450 students and about 50 instructors and other staff were evacuated from the campus. A daycare center on the campus was also evacuated and the children were sent home with their parents. John Muir Elementary School was also placed under lock down moments before the explosion.
Source: http://latimesblogs.latimes.com/lanow/2010/09/grenade-glendale-los-angeles-sheriffs-department.html

40. *September 2, WJHG 7 Panama City* – (North Carolina; Florida) **Hurricane Earl: F-15's evacuate to Eglin Air Force base.** The threat of high winds associated with Hurricane Earl forced pilots on a fleet of 35 F-15 Strike Eagles and 3-KC-135 stratotankers to evacuate from Seymour Johnson Air Force Base in Goldsboro, North Carolina. They are waiting out the storm at Eglin Air Force Base in Valparaiso, Florida, which is only a 1 hour and 15 minute flight away. Jets began arriving in groups of four around 10:30 a.m. September 2 and will be housed on the 33rd fighter wing flightline that was originally built for the incoming F-35 jets. At best, the squadron will be heading home September 3, depending on the path and destruction of the hurricane.
Source: http://www.wjhg.com/home/headlines/102120524.html

41. *September 2, Washington Post* – (Virginia) **McDonnell: Some data may be lost as a result of computer outage.** The governor of Virginia said September 2 that it is possible some data may be lost due to a statewide computer outage this week that affected 26 state agencies, including the Department of Motor Vehicles (DMV). The problem began August 25 with the crash of a pair of 3-year-old memory cards — one was supposed to back up another. The governor told Northrop Grumman CEO that he wanted his company — who holds a $2.4-billion contract with the state — to restore as much data as possible. The contractor's chief information officer said Northrop Grumman will be fined in excess of $100,000, but the amount will be calculated to include the costs of overtime for state employees including the DMV, which will be open this weekend and next.
Source:
http://voices.washingtonpost.com/virginiapolitics/2010/09/giv_bob_mcdonnell_r_there.html?wprss=virginiapolitics

42. *September 2, Gainesville Guardian* – (California; Florida) **P.K. Yonge laptop is stolen with student, employee records.** A laptop containing the personal information of more than 8,300 current and former employees and students of P.K. Yonge Development Research School was stolen last month in San Francisco, California the University of Florida (UF) announced August 31. The computer contained employee payroll, employee parking permit and student information dating back to 2000. It included names, Social Security numbers, and in some cases, driver's license numbers. The laptop was stolen July 23 from a P.K. Yonge employee's rental car while she was on vacation in San Francisco, according to a police report. The files were protected with passwords, but school officials do not know if the information was accessed. UF reported that no credit card information or academic or medical records were on the computer. In an attempt to safeguard against such incidents in the future, P.K. Yonge is installing encryption software on laptops containing sensitive data. Officials mailed letters to 841 people this week to notify them about the breach. More letters are expected to be mailed next week once names and addresses are matched with Social Security and driver's license numbers. School officials do not have contact information for everyone with information on the laptop.
Source: http://www.gainesville.com/article/20100902/GUARDIAN/9021021/1002

For another story, see item **46**

[Return to top]

Emergency Services Sector

43. *August 30, CBS 13 Sacramento* – (California) **Investigations launched into Folsom prison riot.** Folsom State Prison in Folsom, California remains locked down and could stay that way for weeks while authorities investigate the circumstances surrounding the riot that left five inmates wounded from guards' bullets. A Folsom prison lieutenant said the situation exploded when an argument broke out between two men on the handball court in the prison's recreation yard August 27. The verbal altercation turned physical and escalated into a full-fledged melee involving more than 200 inmates. Officials called for backup from nearby California State Prison in Sacramento, to help quell the riot. When the chemical agents had little effect, guards began firing rubber bullets at the participants. When even that failed to stop the brawl, guards used conventional firearms. In all, 60 prisoners were injured. Seven inmates needed hospitalization for their wounds; five from bullet wounds and two from assault injuries. Three inmates remain hospitalized in stable condition. The fight only lasted for 6 minutes, but it took 45 staff members about half an hour to calm the crowd. The investigations into the events leaded up to the riot and the use of potentially lethal force could take weeks, and inmates could remain in lockdown until then.
Source: http://cbs13.com/crime/folsom.prison.riot.2.1887468.html

[Return to top]

Information Technology Sector

44. *September 3, SC Magazine UK* – (International) **SQL injections dominated malware in 2010, as Gumblar botnet named as 'the most significant malware development in years'.** The number of IPS SQL injections increased substantially in the second quarter of 2010 following a downturn. Cisco's global threat report for the second quarter revealed IPS SQL injection signature firings increased substantially in the period to coincide with outbreaks of SQL injection-compromised Web sites. It also claimed Asprox SQL injection attacks made a reappearance in June of 2010, after nearly 6 months of inactivity. A senior security researcher at Cisco said: "SQL reappears in this period, but we can predict with some certainty where the next wave of SQL injections are coming from using our statistics." The report also found that 7.4 percent of all Web-based malware encounters in the first quarter of 2010 resulted from search engine queries, while nearly 90 percent of all Asprox encounters in June of 2010 were the results of links in search engine results pages. The researcher noted the data was collected from actual user clicks, and not overall detections. "This is based on actual users who encountered malware and on actual events ... we are reporting on actual events and I see that as a high figure and the only one that tops it is Gumblar." The Gumblar "botnet" of compromised Web sites was first detected by ScanSafe as a collection of Web sites being used to distribute Web-based malware. Asked if it was still active, the Cisco researcher called it "the most significant malware development in

years." She said: "We took notice of trusted Web sites and the themes on the Web site, and Gumblar took it to a new level with botnets of compromised Web sites."
Source: http://www.scmagazineuk.com/sql-injections-dominated-malware-in-2010-as-gumblar-botnet-named-as-the-most-significant-malware-development-in-years/article/178186/

45. *September 2, Threatpost* – (International) **Google releases Chrome 6 with 14 security updates.** Google has released a new version of its Chrome browser and has included more than a dozen security fixes in the update. The new version, 6.0.472.53, was released 2 years to the day after the company pushed out the first version of Chrome. Google Chrome 6 includes patches 14 total security vulnerabilities, including six high-priority flaws, and the company paid out a total of $4,337 in bug bounties to researchers who reported the vulnerabilities. A number of the flaws that didn't qualify for bug bounties were discovered by members of Google's internal security team. The new release of Chrome also fixes an older bug, a Windows kernel flaw, that Google had thought it fixed in a previous version. The highest bug bounty, $1,337, was paid for the user who discovered an integer error in WebSockets. A second high-priority flaw, a sandbox parameter deserialization error, was discovered by two members of Adobe's Reader Sandbox Team. This is the first major release of Chrome since Google increased the rewards it pays to researchers who identify bugs in the browser. None of the bugs fixed in Chrome 6 qualified for the maximum reward of $3,133.7, which Google said it will pay out for bugs deemed to be SecSeverity Critical.
Source: http://threatpost.com/en_us/blogs/google-releases-chrome-6-14-security-updates-090210

46. *September 2, Compterworld* – (International) **Northrop Grumman takes blame for Va. IT services outage.** Northrop Grumman September 2 apologized for an outage that began August 24 and caused 26 Virginia state agencies to lose their Web services, some for more than 1 week. "Northrop Grumman deeply regrets the disruption and inconvenience this has caused state agencies and Virginia citizens," the president of Northrop Grumman Information Systems, said in a statement. The Virginia Information Technologies Agency (VITA) outsources the management of its data centers to Northrop Grumman through a 10-year, $2.4 billion contract that it signed in 2005. The outage affected 13 percent of the Commonwealth's file servers. VITA's contract with Northrop Grumman has been criticized in the past for a number of project delays, cost overruns and performance problems that included other service outages. Virginia's governor has called for an outside investigation of the latest incident. On August 25, the failure of a storage area network (SAN) caused Web site outages at 26 of Virginia's 83 state agencies. As of August 31, all but three agency sites had been restored, leaving the commonwealth's Department of Motor Vehicles (DMV), the Department of Taxation and the state Board of Elections without services. At the root of the outage was an EMC DMX-3 storage array — the vendor's flagship product, according to published reports. On September 1, the president of Northrop Grumman Information Systems said the failure wasn't so much the memory card as it was the system in place to back it up. The company indicated it supports an independent inquiry and noted it would reimburse Virginia "for the reasonable costs of an assessment."

Source:
http://www.computerworld.com/s/article/9183460/Northrop_Grumman_takes_blame_for_Va._IT_services_outage

47. *September 2, IDG News Service* – (International) **Hotmail suffers hours-long outage on Thursday.** A technical problem kept an undetermined number of Windows Live Hotmail users locked out of their e-mail accounts for hours September 2. The problem, which started at around 3:30 a.m. U.S. Eastern Time, has affected "a small amount of customers," a spokeswoman for Microsoft said via e-mail. She declined to be more specific about the number of people affected. "We are continuing to investigate the issue, but can confirm that the majority of customers that were affected are now able to access their Hotmail accounts," she wrote. The outage apparently was large enough to warrant the posting of a prominent note at the top of the Windows Live Solution Center stating that Hotmail is experiencing lo-gin issues. The message remained on the page as of 7 p.m. September 2, meaning the problem is now entering approximately its 16th hour. Hotmail has about 355 million active accounts worldwide, the spokeswoman said, citing figures from comScore.
Source:
http://www.pcworld.com/businesscenter/article/204794/hotmail_suffers_hourslong_outage_on_thursday.html

48. *September 2, DarkReading* – (National) **IPv6 transition poses new security threats.** The countdown to the saturation of the IPv4 address supply is now down to a matter of months: and along with the vast address space of the next-generation IPv6 architecture comes more built-in network security as well as some new potential security threats. IPv6 has been in the works for over a decade now, but with the exhaustion of the IPv4 address space expected anywhere from spring to June of 2011, the long transition to the new IP may finally be on the radar screen for some organizations. Unlike its predecessor, the "new" protocol was built with security in mind: it comes with IPSec encryption, for instance, and its massive address space could help prevent worms from propagating, security experts said. But its adoption also poses new security issues, everything from distributed denial-of-service (DDoS) attacks to new vulnerabilities in IPv6 to misconfigurations that expose security holes. Some experts expect implementing DNSSEC in an IPv6 network to be simpler than in existing IPv4 networks. "It eases the transition to DNSSEC. IPv6 lets you migrate to DNSSEC much more easily than trying to do so on an old IPv4 stack. The concern with DNSSEC has been you've got a lot of legacy IPv4 equipment out there, and some of it is non-standard, which is very difficult" to integrate with DNSSEC, said the COO of Lumeta.
Source:
http://www.darkreading.com/vulnerability_management/security/perimeter/showArticle.jhtml?articleID=227300083&subSection=Perimeter+Security

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

49. *September 3, ChicagoNow* – (Illinois) **US Cellular customers lose Bus Tracker texting service.** A US Cellular customer had problems getting Bus Tracker text alerts to his phone September 2. He wrote to Chicago Transit Authority customer service and got this response: "US Cellular customers are currently unable to use 41411 as of right now, due to a temporary outage between our vendor and US Cellular. However, you will regain access next week." It turns out that the problem is not with the CTA Bus Tracker program. It seems that US Cellular customers are temporarily blocked from using any services supported by TextMarks, including CTA Bus Tracker two-way texting, said the spokesperson. TextMarks allows companies, churches and agencies like the CTA to communicate with large groups using a keyword. For the CTA, cell phone users can text CTABUS with the four-digit bus stop identifier, such as "CTABUS 5926" to the TextMark number 41411. The CTA would return next-bus time information for the northbound #8 Halsted at Halsted and 14 Place. "CTA first learned of this blockage when the complaint was received through CTA Customer Service," the spokesperson noted. "It appears that US Cellular customers were blocked from TextMarks services beginning August 26 and are expected to have access restored sometime next week."
Source: http://www.chicagonow.com/blogs/cta-tattler/2010/09/us-cellular.html

50. *September 1, The Register* – (National) **Feds crack phone clone scam that cost Sprint $15m.** Federal prosecutors have uncovered a scam that used tens of thousands of cloned cellphones to defraud Sprint out of $15 million in lost long distance revenue. The operation dates back to at least the latter half of 2009, when cellular customers began complaining that they were billed for international calls they didn't make, according to court documents made public September 1. When Sprint employees looked into the matter, they discovered that many of the calls were made from hundreds of miles away from where the customers lived and within minutes of other calls made from the customers' homes. Eventually, the Sprint investigators discovered that electronic credentials were used to make international calls that would have cost $15 million had they been billed at the going rate. What is more, many of the defrauded customers' online accounts were breached so that changes could be made to passwords, international calling features and other settings. The fraud came to light in a criminal complaint that accused nine Sprint employees of illegally accessing customer accounts more than 16,000 times between January and June of 2010. Among the information they took were the MSID, or mobile station ID, and the ESN, or electronic serial

number, that are used to uniquely identify each handset on the Sprint network. By plugging the credentials into new cellphones, people were able to make phone calls that were charged to the accounts of the defrauded customers.
Source: http://www.theregister.co.uk/2010/09/01/sprint_phone_cloning_scam/

[Return to top]

Commercial Facilities Sector

51. *September 3, Daytona Beach News-Journal* – (Florida) **Suspicious package closes park.** Edgewater, Florida city workers found a box containing bottles and aerosol cans at Menard May Park September 2 and called police. An officer with military experience in Iraq indicated the package was suspicious. "The fuse coming out of it was a hint," one officer said. Six hours later, police rendered the device safe with a small, controlled blast. No one was hurt. Investigators have "indicators that it was" a bomb but were conducting lab tests on debris. The Bureau of Alcohol, Tobacco, Firearms and Explosives and local police were working together to identify "who built the device and what it was intended to do."
Source: http://www.news-journalonline.com/news/local/southeast-volusia/2010/09/03/suspicious-package-closes-park.html

52. *September 2, KTEN 10 Ada* – (Oklahoma) **Suspicious device found in Ardmore church.** On September 2, the bomb squad was called in Ardmore, Oklahoma, after authorities say an improvised explosive device was left in the parking lot of Northwest Baptist Church. The bomb squad destroyed the device. No one was hurt, and there were no evacuations. So far, no suspects have been arrested. The Ardmore Police and the Oklahoma Highway Patrol Bomb Squad are still investigating.
Source: http://www.kten.com/Global/story.asp?S=13093544

53. *September 2, KOAT 7 Albuquerque* – (New Mexico) **Apt. complex evacuated after pipe bomb discovery.** Ten units in the Arrowhead Ridge apartment complex in Rio Rancho, New Mexico were evacuated September 2 after police found two pipe bombs after serving a search warrant just after midnight to an apartment for narcotics. A bomb squad was asked to come and remove the devices and detonate them in a safe manner. Officers also found a significant amount of marijuana and cocaine in addition to cash and guns. Residents were able to return home by 10 a.m.
Source: http://www.koat.com/r/24853694/detail.html

[Return to top]

National Monuments and Icons Sector

54. *September 3, Associated Press* – (West Virginia) **W.Va. says DNR site has 500K tons of explosives.** A West Virginia official said authorities have found more than 500,000 pounds of explosives in rented bunkers at the McClintic Wildlife Management Area near Point Pleasant. The deputy state fire marshal said September 2 that officials are

trying to determine how to clean up the area, where stored gunpowder exploded last May. The Army has warned officials to be extremely cautious because some of the explosives are unstable. The state Division of Natural Resources (DNR) recently closed 305 acres of the area because of the potential for fire or explosion. During World War II, the U.S. Army built several concrete bunkers on the property to store munitions. The DNR now owns the bunkers and leases them for storage.
Source: http://www.dailymail.com/News/201009030252

55. *September 3, WHDH 7 Boston* – (Massachusetts) **Campers evacuate as Cape prepares for Earl.** Residents in Cape Cod, Massachusetts took final preparations September 2 for the impending arrival of Hurricane Earl. Even after the sun went down the work continued as people pulled their boats from the water before the hurricane arrived. At Ryders Cove in Chatham, more than 150 boats were pulled from the water September 2. Campers were forced to leave Nickerson State Park in Brewster by 5 p.m. September 2 as Earl approaches. The American Red Cross is prepared in case they need to put up some shelters along Cape Cod, and if necessary, they could house up to 10,000 people a night.
Source: http://www1.whdh.com/news/articles/local/12002115827857/campers-evacuate-as-cape-prepares-for-earl/

56. *September 2, XETV 6 San Diego* – (California) **Brush fire fought on Pacific Crest Trail; Campo School evacuated.** Firefighters hoped that cool coastal air overnight would help calm the wildfire that has chewed through 719 acres of rural San Diego County, California. A California Department of Forestry and Fire Protection spokesman said the fire, which broke out September 2, prompted a precautionary evacuation of an elementary school in Campo about 50 miles east of San Diego. The fire is 10 percent contained. The so-called Cowboy fire was approaching Star Ranch, which is home to horses and cattle and is the proposed site of a housing development but there are no structures in the immediate area. A team of engines was staged at the ranch to protect its structures. Ten fire engines, five fire crews, three helicopters, one helitanker, six airtankers and a bulldozer responded to battle the blaze. Winds died down as night fell, but the National Weather Service predicts that strong high pressure would bring increasing heat in the inland region September 3.
Source: http://www.sandiego6.com/news/local/story/Brush-Fire-Fought-on-Pacific-Crest-Trail-Campo/XDyNcAJry0KzEe3nBxDbRA.cspx

57. *September 2, Associated Press* – (Maryland) **Officials evacuate Assateague campground.** Officials have evacuated the campground at the Assateague Island National Seashore in Maryland ahead of strong winds and rain expected from Hurricane Earl. Officials evacuated the campground September 2, and ordered visitors off of the beach starting at 6 p.m. September 2 through September 3. Onlookers described an unusual migration of the island's wild horses, which have apparently moved on their own because of the weather. Meanwhile, Assateague State Park remained open.
Source: http://www.sfexaminer.com/nation/officials-evacuate-assateague-campground-102095748.html

[Return to top]

Dams Sector

58. *September 3, Laconia Citizen* – (New Hampshire) **Oil from Avery Dam power plant leaks into river, flows downstream.** An undetermined amount of machine lubricant leaked into the Winnipesaukee River near Laconia, New Hampshire September 2. A water boom was stretched across the Winnipesaukee River in Laconia after city officials were notified about oil in the water. Around 10 a.m., the Laconia Fire Department was dispatched to the area along Beacon Street. Fire officials said the caller had seen an oil sheen. Once on scene, firefighters noticed the sheen covering a significant area. The source of the fluid was traced back to just below the dam behind city hall. According to the Laconia deputy fire chief, the oil had come from the turbines inside of the dam house. She said it was likely that one of the oil lines connected to one of the turbines may have broken off. The New Hampshire Department of Environmental Services was called out to analyze the situation to try and access the amount of oil that had leaked. The fire department was not sure how much oil leaked, because 2 hours passed between the initial call and boom placement. The boom setup included several pads, measuring between 8 to 10 inches, made of absorbent material. Source: http://www.citizen.com/apps/pbcs.dll/article?AID=/20100903/GJNEWS02/709039857/-1/CITNEWS08

59. *September 3, Associated Press* – (Virginia) **Virginia residents worry about 'high hazard' dam.** The people who live in the homes and cabins along the Maury River in Rockbridge County, Virginia, are fairly certain of this: If the 44-year-old Goshen Dam ever breaks, the massive wall of water and rock that will wash through their community will kill folks. And, increasingly, they want to know why nobody seems to be doing anything to prepare for that possibility — especially since the federal government concluded more than 30 years ago that the big earthen dam is a "high hazard.'' The government followed up that assessment earlier this decade with a report the dam is "at risk of failure'' if a once-in-200-years storm hits. The U.S. Army Corps of Engineers report concluded that failure of the dam, one of about 30 "high hazard'' dams in the state, would potentially kill 28 people, threaten 265 and cause $25 million in damage along the stretch of river from the dam to Rockbridge Baths. (The Corps calculated there are 165 structures and 330 vehicles in the area's flood plain.) The federal government agreed to "repair and upgrade'' the privately owned dam in 1996, only to fail to do the work. The dam, 38 feet high and 1,300 feet long, holds back the Little Calfpasture River before it merges with the Calfpasture River to become the Maury. Though the dam has always been private property, in 1996 it was included in the Water Resources Development Act, a law that spelled out which U.S. dams would get federally funded upgrades. Work on the damwas priced at $6 million, though the Corps reported in 2006 that it could put "concrete armor'' over the dam at a cost of $5 million. But despite various appropriations over the years, Congress has never fully funded the work, said a Corps of Engineers project manager in Norfolk. Source: http://www.claimsjournal.com/news/east/2010/09/03/113007.htm

60. *September 2, WFAA 8 Dallas-Fort Worth* – (Texas) **Study: Lewisville Lake dam is 'very high risk'.** The U.S. Army Corps of Engineers is calling the Lewisville Lake dam in Lewisville, Texas a "very high risk." The assessment is based on several factors — including the dam's age and the catastrophic consequences downstream if it ever failed. The Corps said lives could be lost in addition to the economic and environmental impact. That is troubling for communities south of the dam, including Carrollton, Farmers Branch, and Dallas. Army Corps officials stress the dam is not in imminent danger of failing. "With any dam, if you did have a failure and you released the pool that was behind the dam, you would have severe flooding along the channel downstream of that dam," said the manager of the lake for the Corps. There are no plans to lower the lake level to prevent problems. The Corps will continue to take a closer look at the dam. Its recommendations are expected sometime next year. Source: http://www.wfaa.com/news/local/Lewisville-Lake-dam-labeled-very-high-risk-102119474.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at 703-872-2267
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

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