Homeland Security
Daily Open Source Infrastructure Report for 8 October 2010

Top Stories

- According to CNN, the Nuclear Regulatory Commission said it plans to improve security procedures in the wake of an investigation into an al Qaeda suspect’s 6 years of employment at several U.S. nuclear power plants. (See item 6)
- The FBI announced that 89 law enforcement officers and 42 others in Puerto Rico were indicted for drug trafficking crimes October 6 in the largest police corruption investigation in the history of the agency. (See item 35)

Fast Jump Menu

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

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

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

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. October 7, Technology Review – (National) How to hack the power grid for fun and profit. The decades-old technology used to manage the power grid is vulnerable to manipulation or sabotage, according to a study revealed this week. Attackers could manipulate power-grid data by breaking into substations and intercepting communications between substations, grid operators, and electricity suppliers. This data is used by grid operators to set prices for electricity and to balance supply and
demand, the researchers said. Grid hackers could make millions of dollars at the expense of electricity consumers by influencing electricity markets. They could also make the grid unstable, causing blackouts. The attacks would be difficult to trace, according to an assistant professor of electrical and computer engineering at Texas A&M University, speaking at the IEEE SmartGridComm2010 conference in Gaithersburg, Maryland. Vulnerabilities have existed in grid systems for decades. But the threat is becoming worse as more substations become automated, and unmanned, making it easier for an attacker to access grid data. As utilities move to open communications standards as part of the migration to the “smart grid,” it could get even easier to intercept communications or hack into systems remotely.

Source: http://www.technologyreview.com/energy/26472/

2. October 7, The Associated Press – (Indiana) Gas leak forces evacuations in South Bend, Ind. A break in a high-pressure natural gas line has forced the evacuation of a four-square-block area of downtown South Bend, Indiana, and left rush-hour traffic snarled. A police captain said the break was reported about 8:20 a.m. October 7. He said it is not known how long it will take to cap the leak. He said some buildings will likely remain closed for hours until authorities can check them for gas. A Northern Indiana Public Service Co. spokesman said the line was damaged by a contractor working on a street project. Among the buildings evacuated are the city-county building and the St. Joseph County Courthouse. Police have routed traffic away from the area, causing traffic tie-ups throughout the city.

Source: http://www.google.com/hostednews/ap/article/ALeqM5gTchpyKTyWbtE6l6Bl6P15qYhxgD91MTGB00?docId=D91MTGB00

3. October 7, KIRO 7 Seattle – (Washington) Power outage affects 5,100 across beacon hill. A power outage in the Beacon Hill area of Seattle, Washington affected up to 5,100 Seattle City Light customers October 7, Seattle City Light said. The boundaries of the outage were South Alaska Street to the north, South Norfolk Street to the south, Lake Washington to the east, and Airport Way South to the west. The outage began at about 1:30 a.m. and by 2:15 a.m., crews reduced the outage to 2,000 customers. At that time, the public utility department did not yet know the cause of the outage.


4. October 5, Associated Press – (California) Gas pipe explosion may have been caused by weld or weak section. Experts said a weld or weak section may have caused catastrophic failure of the 54-year-old natural gas pipeline that exploded in flames 3 weeks ago killing 8 people and destroying 37 homes in San Bruno, California. Stanford University’s mechanical engineering department chairman said the pipe “unpeeled and failed catastrophically.” The experts suggested brittle pipes, old welds, corrosion or widening cracks could have caused the failure.

Source: http://www.kypost.com/dpp/news/national/Pipeline-ExplosionCatastrophic-Failure

For another story, see item 24
Chemical Industry Sector

5. **October 6, Abilene Reporter-News** – (Texas) **Snyder man burned in chemical blast.** An investigation continues into a chemical company explosion and flash fire that injured a 50-year-old Snyder, Texas, man. He suffered second- and third-degree burns in the accident that occurred at an oil field chemical company the night of October 4, officials at the Snyder Fire Department reported. The explosion occurred at 7:34 p.m. at a facility owned by Chemplex LC in the 100 block of North Old Lubbock Highway. The man, who was an employee of the company, sustained burns over 45 percent of his body, said the Snyder fire marshal. The explosion occurred as workers were mixing chemicals.

6. **October 6, St. Petersburg Times** – (Florida) **Semi driver killed after truck rolls over, catches fire in Plant City.** A semitrailer truck driver was killed October 6 after the vehicle struck a concrete pole, flipped and caught fire, according to Plant City, Florida, police. The crash happened around 12:15 a.m. near Trapnell Road and Highway 39. The truck was carrying fertilizer, and some of the contents caught fire and spilled on the road. The 60-year-old driver veered off the road after having a medical issue, officials said. Officials said the road will be blocked for several hours.

Nuclear Reactors, Materials and Waste Sector

7. **October 6, CNN** – (National) **Al Qaeda suspect at nuke plants leads to promise of improved security.** The Nuclear Regulatory Commission said it plans to improve security procedures in the wake of an investigation into an al Qaeda suspect’s employment at several U.S. nuclear power plants. The investigation by the commission’s inspector general was carried out at the request of two New York Congressional Democrats, after it emerged that the al Qaeda suspect had worked for 6 years at nuclear power plants in the Northeast, mainly the Salem/Hope Creek plant in New Jersey. The inspector general’s report, which is heavily redacted for security reasons, said the suspect’s had unescorted access to the sites where he worked. However, it notes he did not have access to “safeguards information” or computer systems. The commission defines safeguards information as that likely to have “a significant adverse effect on the health and safety of the public” if disclosed. The inspector general’s report said the suspect’s behavior should have raised suspicions.


8. October 6, Global Security Newswire – (Wyoming) GOP lawmakers hope to halt Uranium mine deal. Four senior Republican lawmakers pressed the Presidential Administration October 5 to squelch a proposed deal that would give the Russian state-run atomic energy firm Rosatom control of a Wyoming uranium mine and processing site, the Washington Times reported. The potential deal would give Atomredmetzoloto, a branch of Rosatom, a 51 percent share of Uranium One USA Inc., operator of the Powder River Basin site in Wyoming. The Russian entity currently holds 23.1 percent of the Canadian-based firm’s common stock, according to a company fact sheet. The transaction, announced August 31 and slated for completion in 2010, must still receive backing from the Nuclear Regulatory Commission and the interagency Foreign Investment in the United States Committee. Source: http://www.globalsecuritynewswire.org/gsn/nw_20101006_8705.php

9. Critical Manufacturing Sector

October 6, Aviation Web – (National) FAA mandates upgrade to Eclipse avionics. “Uncommanded changes” to radio frequencies, altitudes and transponder codes by the electronic flight information systems in some Eclipse jets have been reported, the Federal Aviation Administration (FAA) said, and an Airworthiness Directive (AD) issued this week mandates upgrades to the system. The AD affects approximately 168 aircraft in the fleet, the FAA said, and depending what kind of system the airplane has, the fix could cost as little as $770 to $1,670, or as much as $249,950. The FAA said it has “no way of knowing” how many airplanes would need each type of upgrade. Eclipse Aerospace said the AD is related to a 3-year-old Service Bulletin originally issued by Eclipse Aviation. “Eclipse Aerospace has verified that 90 percent of the fleet has previously complied with the service bulletin,” the statement said. “By issuing this AD, the FAA is ensuring that the other 10 percent of the fleet complies ... Eclipse Aerospace supports the FAA’s adoption of this AD and encourages all remaining operators to comply with its requirements.” Source: http://www.avweb.com/avwebflash/news/FAAMandatesUpgradeToEclipseAvionics_203395-1.html

10. October 6, Suburban Journals – (Illinois) No dangerous fumes detected around Venice factory blaze. An air monitoring center about 2 miles from the site of Venice, Illinois factory fire detected no increase in dangerous chemicals after a fire at a magnesium plant October 4, the state environmental protection agency reported. The fire at Magnesium Elektron sent smoke across Venice and surrounding neighborhoods. Some worried the smoke was toxic. State environmental officials are working with the Illinois Department of Public Health and the Agency for Toxic Substances and Disease Registry to evaluate possible health issues. The agency said in a release that “information currently available to the Illinois EPA does not indicate any potentially negative impact to the health of area citizens, especially considering the short time anyone might have been exposed.” Magnesium was the primary chemical in the fire.
Defense Industrial Base Sector

11. October 7, Military Times – (National) **Test F-35s return to the air.** Lockheed’s F-35 Lightning II test planes are flying again after being grounded last week due to software glitches involving the jets’ fuel pumps, company officials have confirmed. “Over the weekend, we loaded the software solution onto the flight test aircraft,” a company spokesman said October 5. While the conventional takeoff F-35As are cleared to fly, the short-takeoff-and-vertical-landing (STOVL) F-35Bs have yet to receive clearance. Additional problems with the B model’s auxiliary inlet door are keeping those jets on the ground, according to the company. “The F-35B jets are still restricted to CTOL-mode only operations, as we implement the corrective actions that address the auxiliary inlet door issue,” the spokesman said.

Banking and Finance Sector

12. October 7, Washington Post – (National) **Loan chaos may pose wider peril.** Millions of U.S. mortgages have been shuttled around the global financial system — sold and resold by firms — without the documents that traditionally prove who legally owns the loans. Now, as many of these loans have fallen into default and banks have sought to seize homes, judges around the country have increasingly ruled that lenders had no right to foreclose, because they lacked clear title. These fundamental concerns over ownership extend beyond those that surfaced over the past 2 weeks amid reports of fraudulent loan documents and corporate “robo-signers.” The court decisions, should they continue to spread, could call into doubt the ownership of mortgages throughout the country, raising urgent challenges for both the real estate market and the wider financial system.
Source: [http://www.washingtonpost.com/wp-dyn/content/article/2010/10/06/AR2010100607245.html](http://www.washingtonpost.com/wp-dyn/content/article/2010/10/06/AR2010100607245.html)

13. October 6, Bank Info Security – (Maryland) **Ex-Fannie Mae contractor convicted.** A federal jury in Maryland convicted a disgruntled software programmer for planting a virus on mortgage giant Fannie Mae’s computer servers in late 2008. The 36-year-old programmer of Montgomery County, was charged with computer intrusion after inserting malicious script. Had the malware not been discovered shortly after the programmer’s termination, it could have shut down Fannie’s systems completely for 1 week or more, and would have cost millions to repair and restore data on the firm’s
nearly 5,000 servers. The programmer, an Indian citizen, had worked as a software engineer at Fannie Mae’s Urbana offices since 2006 and for 3 years was given access to all of the firm’s servers. According to testimony and evidence presented at trial, he was fired October 24, 2008 and told to turn in all of his Fannie Mae equipment, including his laptop. On October 29, a Fannie Mae senior engineer discovered a malicious script embedded in a routine program that was intended to execute January 31, 2009. The FBI agent investigating the case said the programmer allegedly embedded the destructive code, designed to wipe out all data across the network by overwriting the data with zeroes.


14. October 6, Storefront Backtalk – (National) Skim scam: Did Aldi invite 11-state coordinated attacks. When a gang of thieves physically tampers with point-of-sale systems, the tampering is usually a local operation. But that may be changing. Discount grocer Aldi said October 1 it has found tampered payment-card readers in stores in 11 states, spread from the East coast to Illinois. The retailer said the tampering was only in a limited number of its 1,100 U.S. stores, and all those stores were clustered near 10 cities — but the stolen data is being cashed out thousands of miles away. Part of what made the $70 billion global grocery chain so successful could be playing a key role in making it a cyberthief target today: The scarcity of store employees. The 10 areas hit with tampering were Chicago; Indianapolis; Pittsburgh; Philadelphia (including stores in New Jersey); Atlanta; Washington, D.C. (including stores in Virginia and Maryland); Rochester, New York; Hartford, Connecticut; Raleigh, North Carolina; and Charlotte, North Carolina. The retailer said that the skimming devices were probably placed during June, July and August.

Source: http://www.storefrontbacktalk.com/securityfraud/aldi-pin-pads-tampered-with%E2%80%95and-theyre-all-over-the-map/

15. October 6, Bloomberg – (International) Russian cybercrime thrives as Soviet-era schools spawn hackers. The U.S. Department of Justice said it may have been the most sophisticated computer fraud ever. A 29-year-old in September pleaded guilty to participating in a worldwide hacking scheme that led to the illegal withdrawal of more than $9 million from cash machines worldwide operated by RBS WorldPay Inc., the U.S. payment-processing division of Britain’s Royal Bank of Scotland Group Plc. The conviction shed light on a growing trend from Russia. Just as the Russian president seeks to persuade investors his country is a safe place, more technology graduates are turning to cybercrime. The FBI last week charged 37 suspects from Russia, Ukraine and other eastern European countries of using a computer virus to hack into U.S. bank accounts. “The number of hackers reflects how many good engineers we potentially have in this country,” the president of Google Inc. in Russia said in a Bloomberg Television interview in Moscow. Russians committed more than 17,500 computer-related crimes last year, or 25 percent more than in 2008, according to the Interior Ministry’s latest statistics.

Transportation Sector

16. October 7, Gothamist – (New York) **Bronx man arrested for Penn Station bomb threat.** Police arrested a 19-year-old Bronx, New York man October 6 for allegedly threatening to blow up Penn Station and other transit hubs. The man was also arrested last year for threatening to kill the U.S. President and the New York Police Department commissioner. The man allegedly made four calls to the Port Authority tip line. News sources report the man said he was going to set off a grenade in Manhattan’s Penn Station. He also allegedly threaten to blow up Newark Penn Station and the 175th Street station of the A Train. An investigator called the suspect the night of October 5, and police paid a visit to his Bronx home, but he wasn’t home. The suspect called back October 6, and said he was planning to detonate the explosives by the end of the day. The Port Authority’s investigators convinced him to meet them near Yankee Stadium, where he was arrested. He was charged with four counts of aggravated harassment. Source: [http://gothamist.com/2010/10/07/bronx_man_arrested_for_penn_station.php](http://gothamist.com/2010/10/07/bronx_man_arrested_for_penn_station.php)

17. October 6, Portland Oregonian – (Oregon) **Army Corps postpones dredging of hazardous bar in Willamette river.** The Army Corps of Engineers has bumped dredging of a potentially hazardous bar in Portland Harbor to next summer, saying resolving environmental concerns pushed the project too close to the October 31 deadline for completing in-water work. Surveys in June indicated that shoaling on the Post Office Bar reaches across two-thirds of the outbound navigation channel, the Corps’ Portland office said, increasing the chances of vessels running aground or colliding. The bar, 2 miles up the Willamette from its confluence with the Columbia River, was last dredged in 1989. The Corps will monitor the area more frequently, and said it could pursue an emergency dredging project before next summer if necessary. The in-water work deadline is designed to protect salmon listed under the Endangered Species Act. Source: [http://www.oregonlive.com/environment/index.ssf/2010/10/army_corps_postpones_dredging.html](http://www.oregonlive.com/environment/index.ssf/2010/10/army_corps_postpones_dredging.html)

18. October 5, KTXL 40 Sacramento – (California) **FBI investigates laser pointed at CHP and Southwest airplanes.** The FBI is investigating a green laser being pointed at two aircraft in Sacramento, California. Southwest Flight 829 was flying in the area of Hwy 99 and Hwy 50 at 7:41 p.m. the night of October 5 when they reported being hit by a green laser. The California Highway Patrol (CHP) was asked to assist in searching near the Arden Arcade area where they believed the laser was coming from. While CHP’s fixed wing aircraft was in the air, it was also hit by the green laser, CHP officials said. The FBI is now investigating this incident because pointing a laser at an aircraft is a federal crime. Law enforcement officials searched the area but were unable to locate any suspects. Source: [http://www.fox40.com/news/headlines/ktxl-news-laserataircrafts,0,5294007.story](http://www.fox40.com/news/headlines/ktxl-news-laserataircrafts,0,5294007.story)
Postal and Shipping Sector

19. October 5, Topeka Capital-Journal – (Kansas) **Powder sent to Phelps law firm.** FBI laboratory test results on white powder received in the mail October 5 at the Phelps Chartered law office in Topeka, Kansas, were negative, a spokeswoman for the firm said. Based on the results, it is safe for employees to return to the part of the office exposed to the powder, said a lawyer at the firm said. “It was about 11 a.m. [Tuesday] when we opened the mail,” the lawyer said. When an office assistant at Phelps Chartered, 1414 S.W. Topeka Blvd., opened the envelope, the powder “poofed out,” the lawyer said. The room was sealed off, and Topeka police were called, then the fire department’s hazardous materials unit was summoned. Police called the FBI, and an agent went to the office. The office assistant did not suffer any adverse reaction to the powder and did not go to a hospital, the lawyer said. Investigators seized the clothes she was wearing because powder got on them.


Agriculture and Food Sector

20. October 6, New York Times – (National) **Honeybee killer found by Army and entomologists.** A partnership of military scientists and entomologists appears to have achieved a major breakthrough: identifying factors that may be to blame for the loss of 20 to 40 percent of bee colonies in the United States since 2006. A fungus tag-teaming with a virus have apparently interacted to cause the problem, according to a paper by Army scientists in Maryland and bee experts in Montana in the online science journal PLoS One. Exactly how that combination kills bees remains uncertain, the scientists said — a subject for the next round of research. But there are solid clues: both the virus and the fungus proliferate in cool, damp weather, and both do their dirty work in the bee gut, suggesting that insect nutrition is somehow compromised. Research at the University of California, San Francisco, had already identified the fungus as part of the problem. And several RNA-based viruses had been detected as well. But the Army/Montana team, using a new software system developed by the military for analyzing proteins, uncovered a new DNA-based virus, and established a linkage to the fungus, called N. ceranae.


21. October 6, Freeport Journal-Standard – (Illinois) **Feds criticize state EPA handling of big farms.** A federal report critical of the Illinois Environmental Protection Agency (IEPA) has ordered steps be taken to revamp inspection and enforcement of regulations governing confined animal feeding operations (CAFOs). The report could affect how citizen complaints about Traditions Dairy, a proposed large-scale dairy farm near Nora,
Illinois are handled by the IEPA. A petition filed by Illinois Citizens for Clean Air and Water (ICCAW), and other environmental groups, requested an investigation by the U.S. Environmental Protection Agency (EPA) into the IEPA’s oversight of CAFOs. The result was a 2-year-long investigation that culminated in a 41-page report issued last month by EPA. Findings in the report criticized the state agency for failing to gather enough information during its inspections to determine whether large-scale farm operations were complying with water quality regulations. Even after the IEPA identified violations of environmental laws at CAFOs, less than one-half of the farms complied with the recommended enforcement actions set forth by the state agency, the federal report states. The IEPA has also been slow to respond to citizen complaints or take formal enforcement action against CAFOs where alleged violations have been reported, according to EPA.


22. October 5, The Packer – (New York; California) Sprouts recalled in New York and California. Authorities in California and New York are warning consumers against eating certain sprouts products. The California Department of Public Health September 30 issued a warning to consumers about Sacramento, California-based Banner Mountain-branded alfalfa sprouts. The agency said no one has reported getting sick from the product, according to a news release. In New York, after routine sampling by food inspectors and subsequent analysis discovered listeria contamination, an alfalfa supplier is recalling soybean sprout packages from Essex Farm Inc, which does business as Best Farm. Sold only at one New York grocery store, the recalled soybean sprouts were bought in bulk and repacked at the Essex Street Market store.


23. October 5, Urbana Daily Citizen – (Ohio) Some Ohio corn experiencing stalk lodging. Some corn throughout Ohio, already stressed from lack of adequate moisture, is experiencing stalk lodging and stalk rot. “Recent storms accompanied by strong winds have resulted in stalk lodging in localized areas across the state,” said an Ohio State University Extension state agronomist. “The rapid maturation and dry down of the corn this year may affect the crop. We’ve already received reports of kernels falling off ears, reduced shank strength, ears dropping, and exposed ears in some hybrids.” According to the Ohio Agricultural Statistics Service, 36 percent of Ohio corn has been harvested, far ahead of this time in 2009 and the 5-year average. Abnormally dry conditions and hot weather late in the season rapidly matured the crop and drove growers into the fields to harvest up to 3 weeks ahead of schedule.

Source: http://www.urbanacitizen.com/main.asp?SectionID=3&SubSectionID=5&ArticleID=155114

[Return to top]
24. **October 7, Associated Press and St. Louis Public Radio** – (Missouri) **Coast Guard, state DNR investigating tugboat sinking.** State environmental officials and the U-S Coast Guard are investigating the sinking of a tugboat October 6 on the Mississippi River near St. Louis, Missouri. Workers at the scene of the sinking reported seeing a sheen of oil on the river. The tugboat was carrying about 8,700 gallons of diesel fuel when it ran aground and sank. The Missouri Department of Natural Resources has notified public drinking water sources downstream of the sinking, and set a boom around the sheen. There were no reports of injuries. The Coast Guard will determine the cause of the accident, which occurred around 4:30 p.m. October 6. The boat, the MV Bill Pehler, is owned by American River Transportation Co., a company affiliated with agribusiness giant Archer Daniels Midland.

Source: [http://www.publicbroadcasting.net/kwmu/news.newsmain/article/1/0/1710061/St._Louis_Public_Radio_News/Coast_Guard_state_DNR_investigating_tugboat_sinking](http://www.publicbroadcasting.net/kwmu/news.newsmain/article/1/0/1710061/St._Louis_Public_Radio_News/Coast_Guard_state_DNR_investigating_tugboat_sinking)

25. **October 6, WETM 18 Elmira** – (Pennsylvania) **Boiling water advisory.** Officials are warning all users of the Wellsboro Water System in Wellsboro Pennsylvania to boil their water before drinking it. An alert was sent out October 5 while officials were monitoring the conditions of the filtering system. Officials determined that, “the amount of sand in our slow sand water filters is less than the amount required by the Public Water supply Manual.” Officials stated that the condition could allow disease-causing organisms to enter the water system.


26. **October 6, Red Wing Republican Eagle** – (Minnesota) **Vandals target local reservoirs.** Reservoirs in Goodhue County, Minnesota, have been frequent targets of recent vandalism. Since last spring, vandals have damaged property at three city of Red Wing reservoirs, one of them twice. The city’s water supply was not been harmed but public works drained the Sorin’s Bluff Reservoir as a precaution after one of the incidents. The crimes have perplexed authorities, who say they’re unsure if the incidents are related. “It is just vandalism, I hope,” the Red Wing deputy director of utilities said. The first incident occurred at Sorin’s Bluff in April when authorities discovered a hatch was missing from the reservoir. A second incident took place in mid-July when someone tampered with electrical equipment at the Sand Ridge Reservoir. A T-Mobile tower is located at Sand Ridge and it too was affected. Two other acts of property damage occurred at the Hiawatha Hills Reservoir in August, and on September 18 or 19. Authorities discovered that locks and hinges at the reservoir had been tampered with. “Since we’ve had this problem we’ve increased security,” the utilities director said. The city has installed cameras, new locks and alarms at the reservoirs. In addition to beefing up security, city officials have also notified the Minnesota Department of Health and the FBI. A health department spokesperson said similar incidents have been reported across the state. Vandalizing water systems is a federal offense and carries stiff penalties compared to other acts of vandalism or property, he added.

Public Health and Healthcare Sector

27. **October 7, Odessa American** – (Texas) **Cancer center evacuated briefly.** Staff and patients were forced to evacuate the West Texas Cancer Center at 301 N. Washington Ave. in Odessa, Texas after a fire about 11 a.m. October 6, a city dispatcher said. When the fire department arrived, all employees and patients had evacuated, CBS 7 reported. A city dispatcher said the fire stemmed from construction nearby that didn’t damage the building itself even thought it set off an alarm. CBS 7 reported firefighters told them welding caught roofing materials on fire.


Government Facilities Sector

28. **October 7, Dallas Morning News** – (Texas) **Mesquite High School evacuated due to bomb threat.** Mesquite High School in Mesquite, Texas has been evacuated after a bomb threat was called in October 7. “ Apparently a call came in from a pay phone that there was a bomb,” a Mesquite Independent School District spokeswoman said. The call came before school started so “a lot of students weren’t actually there,” she said. Students and staff were sent to the football stadium next to the school as they arrived. The spokeswoman said she did not know how long the school would be closed. She said that the threat was not specific, but “we always take it seriously.” She did not know when the district had last received a threat but it “has been quite a while.” The school, on East Davis Drive, has about 2,700 students and has several buildings. All were being searched.


29. **October 7, Eau Claire Leader-Telegram** – (Wisconsin) **Cadott student charged in bomb threat.** A Cadott, Wisconsin, student accused of making a bomb threat at a high school last week has been charged with a felony in Chippewa County Court. The 17-year-old was charged with one count of creating a bomb scare, which carries a maximum penalty of 3 and one-half years in prison and a $10,000 fine. When authorities searched his locker, they found a pipe that contained marijuana residue, so he was also charged with a misdemeanor for possessing drug paraphernalia. The suspect was 16 when the bomb threat was issued September 28; he turned 17 October 4. The Chippewa County district attorney said he can charge the suspect as an adult because the law looks at what day charges were filed, not what the suspect’s age was at
the time the act was committed. The district attorney noted the handwritten bomb threat was taken seriously and resulted in the cancellation of school that day. Several law enforcement officers combed through the school for hours in an attempt to find a bomb. “It’s an act of terrorism,” the district attorney said. “It will be dealt with seriously.” He previously said bomb threats are expensive endeavors, as fire departments and law enforcement must respond. He once saw a bill from a fire department charging between $4,000 and $5,000 to investigate a bomb threat.

Source: http://www.twincities.com/ci_16277082?nclick_check=1

30. October 7, Associated Press – (Wisconsin) Bomb scare near Biden’s scheduled appearance. The Dane County, Wisconsin Bomb Squad has determined that a suspicious package found outside the location in Madison where the U.S. Vice President was scheduled to appear is not dangerous. Police shut down about a two-block radius after the plastic tube was found outside the Monona Terrace at about 7:25 p.m. October 6. The roads were reopened around 9:30 p.m. after the bomb squad gave the all clear. A passer-by spotted a package they thought was suspicious and called police. The Vice President was scheduled to speak at the Monona Terrace October 7 at a campaign stop for the Democratic gubernatorial candidate.


31. October 6, Global Security Newswire – (Nevada) Robots to guard Nevada national security site. The Nevada National Security Site (NNSS) plans to deploy three robots to patrol the far reaches of the former nuclear weapons testing installation, the U.S. National Nuclear Security Administration (NNSA) announced October 4. The first of three Mobile Detection Assessment Response System robots has begun operating at the former Nevada Test Site. The compact units are to be operated from the NNSS command facility. They are programmed to make their rounds at random and are equipped with sensors and video cameras that stream live images to their handlers. Operators would only issue commands when the autonomous robots came across something that required further examination. “The robots are a great addition to the NNSS protective force,” the NNSA Associate Administrator said in released remarks. “The robots allow us to improve security at remote portions of the Nevada National Security Site at reduced costs ... NNSA applauds NNSS in seeking ways [to] improve the way it does business while maintaining the highest security standards.” The units can travel as fast as 20 mph and can operate for over 12 hours without refueling. They monitor obstacles, locks and inventory through “radio frequency identification tags.” The units are anticipated to save $6 million by offsetting security infrastructure costs for motion sensors, cameras, lights and other equipment. They are also expected to save another $1 million yearly on security force and technology upkeep costs.

Source: http://www.globalsecuritynewswire.org/gsn/nw_20101005_6354.php

32. October 6, Associated Press – (New Jersey) Manchester student’s parent is accused of bomb threat that forced school to shut down. Authorities in southern New Jersey say the parent of a high school student is responsible for two recent bomb threats at the school. The latest threat was made in a phone message left the night of October 5. It
forced Manchester Township High School to shut down for nearly 3 hours October 6 as police K-9 units searched the campus. No bomb was found. Manchester police told the Asbury Park Press that the 58-year-old suspect was arrested October 6. Police said the suspect admitted making a similar threat September 22. Police said the suspect offered no motive for making the threats. He faces two counts of causing a false public alarm.


For another story, see item 36

**Emergency Services Sector**

33. October 6, Pasadena Star-News – (California) **New evacuation protocols announced for foothill areas.** New evacuation protocols for potential mudslides and debris flows are now in place in foothill areas affected by the Station Fire, sheriff’s officials said October 6. The modified protocols are designed to get residents’ “maximum cooperation” when evacuation orders are in effect, said the Los Angeles County Sheriff’s Chief at a briefing in Alhambra organized by the multi-agency public outreach program Coordinated Agency Recovery Effort (CARE). The Foothill Incident Command’s color-tiered system, which previously had three alert levels, now has a new orange level, where residents choosing not to evacuate will be asked to sign a Refusal to Evacuate Form, which acknowledges their awareness of the hazards and assumes all liability for the decision to remain in place, the sheriff’s chief said.


34. October 6, St. Petersburg Times – (Florida) **Priority dispatch proposal aims to alter Pinellas EMS response system.** Some people could wait longer for help under a proposal that would change the way Pinellas, Florida dispatches its emergency medical personnel. The change, which affects only calls about emergencies that aren’t life-threatening, could be a first step to a total revamp of Pinellas’ EMS response system. The system, known as priority dispatch, is designed to cut down on duplication of services. But it’s unclear whether the move will save any money. Pinellas has not analyzed the possible savings, said the county’s EMS division manager. When someone calls 911 for a medical emergency under the current system, paramedics from one of the county’s 18 fire departments are sent. Also sent are paramedics in a Sunstar ambulance. Under the proposal, which is expected to kick in around December 1, some callers would see only the firefighter/paramedics; others would see only ambulance paramedics; and most would continue to see both.


35. October 6, Federal Bureau of Investigation – (Puerto Rico) **Eighty-nine law enforcement officers and 42 others indicted for drug trafficking crimes.** Eighty-nine law enforcement officers and 44 others in Puerto Rico have been charged in 26
indictments unsealed October 6 and returned by a grand jury in San Juan, Puerto Rico, during the month of September 2010, the U.S. Attorney General and a U.S. attorney for the District of Puerto Rico announced October 6. The defendants face charges ranging from conspiracy to possess with intent to distribute more than 5 kilograms of cocaine, attempt to possess with intent to distribute more than 5 kilograms of cocaine, and use of a firearm during the commission of a drug trafficking offense. The offenses charged cover a period from in or about July 26, 2008 until September 21, 2010. The arrests are the result of Operation Guard Shack, the largest police corruption investigation in the history of the FBI. Close to 750 FBI agents were flown in to Puerto Rico from across the country to assist in the arrests. Currently 129 individuals are in custody and four subjects remain at-large.

Source: http://sanjuan.fbi.gov/dojpressrel/pressrel10/sj100610.htm

36. October 4, KATV 7 Little Rock – (Arkansas) **Mass disaster simulation.** University of Arkansas Medical Sciences (UAMS) emergency room medical teams and the National Guard worked together to simulate a tragedy involving a C-130 crash and mass casualty event at Camp Robinson October 4. “The hardest part and the most crucial part is determining where these patients need to go,” said the UAMS clinical services manager. He helped triage the patients being strolled in on stretches from Lacota and Blackhawk helicopters. Doctors and nurses started organizing patients and they were then sent down on an elevator to the appropriate hospital departments. The injuries ranged from critical to the “walking wounded.”


37. October 7, Cnet News – (National) **Keeping the masses safe on the Internet.** Recognizing that all the technology in the world cannot protect the Internet from attacks, the security industry is targeting an education campaign at the weakest link — computer users. It is the first public service message of its kind in the United States and it’s simple: Stop. Think. Connect. The campaign was unveiled October 7 at Intel headquarters in California. It is part of Cyber Security Awareness Month, an annual event since October 2001, and was organized by the National Cyber Security Alliance, the Anti-Phishing Working Group (APWG) and more than two dozen government agencies and companies including Microsoft, Google, PayPal, RSA, Facebook, Visa, and Wal-Mart. The goal is to get security precautions to become second nature. A security frame of mind must be built into the culture of society and starting at the ground level with end users, said the deputy undersecretary for the national protection and programs directorate at DHS, speaking in a keynote address at the event.


38. October 7, The New New Internet – (International) **Anonymous strikes again; DDoS attacks Spain’s copyright society.** After recently cyber assaulting anti-piracy
advocates and threatening to attack until it “stops being angry,” hacker collective Anonymous has struck again. PandaLabs reported that Anonymous October 6 launched a DDoS attack against the Spanish copyright protection society. As of 2:30 p.m. October 7, PandaLabs had witnessed more than 20 service interruptions to the society’s site, as well as four interruptions to a second Spanish site. In a public statement to the media, Anonymous said: “The SGAE has a slogan ‘Believe in culture,’ while they restrict new creativity by preventing that creativity is shared. They lobbied this Canon Law, which states that suspected piracy websites can be taken down without a court order. This is a danger to freedom of speech, since any site can just be taken down with the excuse that intellectual property is hosted. The ‘Ministerio of Cultura’ should get a message that their current course will only lead to more controversy and protest.” While some have dubbed Anonymous “Internet griefers” and a “hate group,” PandaLabs calls the group’s actions an example of the first organized mass cyber protest on the Internet against entities that work to promote and enforce anti-piracy and copyright laws.


39. October 7, ComputerWorld – (International) Microsoft pitches PC isolation ward to defeat botnets. Microsoft’s security chief October 6 pitched a plan that would block some botnet-infected computers from connecting to the Internet. A noted botnet researcher said the proposal did not attack the problem at its root, and like many technical solutions, was unlikely to do much good. In a paper published October 6, the individual who heads Microsoft’s trustworthy computing group, spelled out a concept of “collective defense” that he said was modeled after public health measures like vaccinations and quarantines. Under the proposal, PCs would be issued a “health certificate” that showed whether the system was fully patched, that it was running security software and a firewall, and that it was malware-free. Machines with deficiencies would require patching or an antivirus update, while bot-infected PCs might be barred from the Internet. Quarantining PCs could be a last-step measure to keep compromised PCs from threatening others on the Web.

Source: http://www.computerworld.com/s/article/9189838/Microsoft_pitches_PC_isolation_ward_to_defeat_botnets

40. October 7, Help Net Security – (International) The threat behind fake LinkedIn messages. Retarus sent out a warning in response to a current wave of fake contact requests via the social media platform LinkedIn. These well-simulated e-mail messages present a considerable risk to PC-owners. Unsuspecting users are lured into a trap via the seemingly well-intentioned e-mails and their PCs are infected with malware in an attempt to gain access to personal information. The e-mails feign to be a contact request sent from the social media platform LinkedIn. Users who try to access the platform via the link are routed to an intermediary Website — with the simple notification “Please waiting ... 4 seconds”. From there, they are then redirected to Google. In these 4 seconds the spyware ZeuS is uploaded in the background and secretly installed. Cyber criminals use this type of spam to gain access to personal information, such as access
data for online banking. Social media spam is on the increase. Retarus analyses have shown that one in three spam e-mails are clearly sent in the guise of social networks. The managing director of Retarus warns, “Social media spam is particularly dangerous because the contents seem well-intended, and the original e-mails are so perfectly imitated, that lay persons are unable to identify them as fakes. Mail users who have defined social media platforms as safe senders, via whitelist entries in their spam filters, are especially affected.”
Source: http://www.net-security.org/malware_news.php?id=1489

41. October 7, TrendLabs Malware Blog – (International) **File infector uses domain generation technique like DOWNAD/Conficker.** Trend Micro has received reports from users about a new, dangerous file infector. This threat, detected as PE_LICAT.A, uses a domain generation algorithm, a technique last seen in WORM_DOWNAD/Conficker variants. This technique allows the file infector to download and execute malicious files from various Internet servers. Like WORM_DOWNAD, PE_LICAT.A generates a list of domain names from which it downloads other malicious files. The domain name generation function is based on a randomizing function, which is computed from the current UTC system date and time. This particular randomizing function returns different results every minute. According to an Escalation engineer, whenever a file infected by PE_LICAT.A is executed, the malware generates a pseudorandom domain name, with the exact value depending on the system’s time. It then tries to connect to the said domain name. If it is successful, it downloads and executes the file at that pseudorandom URL. If not, it tries up to 800 times, generating a “new” URL every time. This helps ensure that the malware will be able to keep itself updated and even if one or more domains are taken offline, others can take its place.

42. October 6, DarkReading – (National) **Fed study: 85 percent of agencies still not using CyberScope.** CyberScope is supposed to be the federal government’s new standard tool for continuous security monitoring. So far, however, the vast majority of federal CIOs said they don’t understand the technology’s mission and goals, and only 15 percent have used it at all. The deadline for filing FISMA security compliance reports using the new CyberScope tool is November 15. According to a study published this week by MeriTalk, a government IT community, the few agencies that have implemented CyberScope give the tool high marks. But 85 percent of the federal IT executives surveyed said they have not deployed it yet. In fact, 72 percent of federal IT executives surveyed said they do not have a clear understanding of CyberScope’s mission and goals. Ninety percent do not have a clear understanding of the submission requirements. The survey results may surprise some in the federal IT space, where some agencies have begun to eschew complex, paper-based FISMA security compliance reporting projects in favor of the “continuous monitoring” concept, where CyberScope provides key functionality. Some 69 percent of survey respondents said they are unsure if this new approach will result in more secure federal networks. The report, underwritten by ArcSight, Brocade, Guidance Software, McAfee, Netezza, and
immixGroup, suggests the Office of Management and Budget (OMB) “must increase communication, clarify submission requirements, and provide training for the reporting protocol shift in order to achieve CyberScope’s goals of enhanced oversight and reporting simplification.”


43. October 6, The Register – (International) **Facebook unveils changes to enhance privacy.** Facebook October 6 rolled out new features designed to make people feel more comfortable putting photos, videos, and other personal data online. In a blog post, the Facebook CEO unveiled an overhauled version of Facebook Groups that allows users to share certain content with select people, rather than with everyone listed as a friend. Vacation photos, for instance, might be shared only with family members, and a team roster might be shared only with other members of one’s Fantasy Football league. It was one of three features the CEO announced. Also unveiled was a new dashboard that tells users at a glance how various Facebook apps are using their data. The panel shows all the apps a user has authorized, what data they use and when the data was last accessed. The CEO also said Facebook was adding a tool that allows users to download everything they’ve ever posted to the social networking site. The photos, wall posts, and other content is archived in a zip file that is downloaded only after a user has entered a password and answered “appropriate security questions.”

Source: http://www.theregister.co.uk/2010/10/06/facebook_groups/

44. October 6, TrendLabs Malware Blog – (International) **EMEA spam growth, APAC infections, in Global 1H 2010 threat report.** Trend Micro has released its Threat Report for the first half of the year. The report focuses on the global trends in online threats. Europe became the largest source of spam globally in the first half of the year. Commercial, scam-based, and pharmaceutical/medical spam accounted for 65 percent of the total number of spam worldwide. HTML spam was the most common kind of spam. There was significant growth in the number of malicious URLs, which increased from 1.5 billion at the start of the year to over 3.5 billion by June. North America was the leading source of these while Asia/Pacific was the region with the most attempts to access these sites. The top URLs blocked by Trend Micro were adult Web sites. Trojan viruses accounted for about 60 percent of the new patterns TrendLabs created in the first half of the year. Overall, 53 percent of the overall number of detections consist of Trojans. Most Trojans lead to data-stealing malware. India and Brazil were identified as the countries with the greatest number of computers that became part of botnets. The bots are used to distribute malware, perpetrate criminal attacks, and send out spam. The full threat report is at TrendWatch under the Threat Reports section.


45. October 6, IDG News Service – (Massachusetts) **Would-be Akamai spy busted by feds.** An Akamai Technologies staffer was arrested October 6 and charged with wire fraud after he provided confidential business information to an undercover federal
agent he believed to be working for an unnamed foreign government. The suspect was charged in federal court October 6 in a case that began in June 2006, when the 42-year-old employee in the finance department of the Cambridge, Massachusetts-based Internet content delivery company sent an e-mail to the consulate of a country referred to only as “country X” in the criminal complaint. In that e-mail, he expressed his desire to help that country with whatever information he could obtain in his position, which he acknowledged was limited to “invoicing and customer contact information.” The foreign consulate the suspect contacted turned his e-mail over to law enforcement authorities, and a little over 1 year later, he was contacted by an FBI agent posing as a representative of “country X.” Over the next 18 months, the suspect left confidential business information such as customer lists and contracts at a designated spot called a dead drop, acts captured via video surveillance. The suspect faces up to 20 years in prison if convicted.

Source:
http://www.computerworld.com/s/article/9189758/Would_be_Akamai_spy_busted_by_feds

46. October 6, The Register – (International) Android phone auto reverts jailbreaks. A new Android smartphone from T-Mobile ships with hardware that thwarts jailbreakers by automatically restoring modified devices to their original factory state. The HTC G2, which began shipping October 5, reinstalls the original firmware when it is rebooted, much to the chagrin of would-be jailbreakers trying to root the device so they can run their own software and third-party applications not approved by T-Mobile. The discovery has generated howls of protest from those who believe that people who buy hardware devices ought to be able to use them however they see fit. Apple has long closed jailbreak holes in iOS updates, and Texas Instruments lobbed legal threats at a hobbyist who posted the cryptographic keys used to modify calculators. Google even has the ability to remotely install or uninstall apps on Android phones. But HTC seems to have upped the ante with a hardware-based approach to meddlesome users who have the gall — and often the expertise — to shun the self-serving restrictions put in place by device and OS manufacturers. It’s not entirely clear how the devices are able to reset themselves. A blogger speculates the new G2 “is using a firmware rewrite system to replace ‘/system’ mods with the ‘official’ firmware upon reboot.” A security researcher tells Threatpost much the same thing. Both say it’s too early to tell if there’s a way to defeat the rollback mechanism.

Source: http://www.theregister.co.uk/2010/10/06/htc_rolls_back_jailbreaks/

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]
47. October 7, Daily Tar Heel – (North Carolina) **UNC sees 110 Wi-Fi locations fail.** The University of North Carolina is trying to find out what caused 110 campus Wi-Fi locations to lose access to the network October 5. The director of university networking systems said the problem began at about 3 p.m. when an engineer from one of the university’s two wireless access point manufacturers made a change on one of the devices. He declined to comment on whether an employee at Cisco Systems, Inc. or Aruba Networks was at fault. The outage lasted from 3 p.m. October 5 to about noon October 6. The report noted the vendor had “never seen that anywhere else before,” and that it was unknown how exactly the outages spread across the network from a single point. “Users should be getting anywhere from 50 to 100 megabytes per second,” he said. “They were only getting around two.” After the outage, network engineers began to visit each affected location and make configuration changes to the access points, according to a summary report sent by the networking systems director. The 110 locations represent a small portion — about 5 percent — of the university’s wireless network, which contains a total of 2,159 wireless access points.


48. October 6, Time – (National) **‘Facebook isn’t working’ as outage hits some users.** Facebook, the social network behemoth, confirmed that unspecified site issues resulted in the site acting slow or unavailable for some of its 500 million users. A spokeswoman wrote an e-mail to the Associated Press October 6 explaining the firm was working on the problem and followed up shortly afterward to say the issue had been resolved.


49. October 6, IDG News Service – (National) **Verizon’s LTE network to reach 38 cities this year.** Verizon Wireless announced that 38 markets, including Los Angeles, Chicago and San Francisco, will get access to the high-speed LTE network by the end of 2010. However, the operator has not yet announced devices that will be able to work on the network. The president and chief operating officer of Verizon made the announcement during a keynote speech at the CTIA conference in San Francisco. The company planned a press conference about the news for October 6. The 38 markets will cover 110 million people “on the day we flip the switch,” he said. He expects the network to offer 8-megabit download speed for users. At launch, the networks will cover on average, 70 percent of the population in each market, he said. Verizon will also launch coverage in 55 airports, he said.

Source: [http://www.computerworld.com/s/article/9189722/Verizon_s_LTE_network_to_reach_38_cities_this_year](http://www.computerworld.com/s/article/9189722/Verizon_s_LTE_network_to_reach_38_cities_this_year)
50. October 6, MyCentralJersey.com – (New Jersey) **Meth lab may have sparked East Brunswick motel explosion, cops say.** Scores of police and firefighters responded to a mid-afternoon explosion October 6 at the Motel 6 off Route 18 in East Brunswick, New Jersey. The emergency responders found a methamphetamine lab gone wrong and a suspect from Kansas. Officers evacuated the motel of about 25 people and arrested the suspect after he fled in a vehicle down lower Edgeboro Road. “We think he was trying to produce methamphetamine,” the incident commander said. Specific charges had not yet been determined as of October 6.

51. October 6, WIS 10 Columbia – (South Carolina) **Walmart bomb threat suspect in custody.** South Carolina’s Richland County deputies said they have a man in custody who they believe is behind a suspicious package found at Jewelry Warehouse on Bower Parkway in Columbia, and a bomb threat at the Walmart on Harbison Boulevard October 6. Around 4:45 a.m., officers recovered an envelope at Jewelry Warehouse containing documents connected to a bomb threat at Walmart. That discovery prompted officers to clear out the store, which was later given the all clear. According to South Carolina Law Enforcement Division officers, that package contained letters outlining “devices” placed around the city. Deputies said a 26-year-old was arrested without incident around 10:30 a.m. in a wooded area on Old Monticello Circle. However, no charges have been filed yet. Officials with the Columbia Police Department, Columbia-Richland Fire Department, SLED, Richland County Sheriff’s Department, and Richland County Emergency Medical Services responded to the store.

52. October 6, KRQE 13 Albuquerque – (New Mexico) **Bomb squad called to hotel.** A report of a suspicious device, described as possibly being a hand grenade, brought the Albuquerque Police Department bomb squad to a Quality Suites hotel in Albuquerque, New Mexico, October 6. Occupants of the hotel were confined to the building, and police were telling motorists and pedestrians to avoid the area. KRQE News 13 reported from the scene that the device turned out to be some type of firework.

For another story, see item 19

[Return to top]

### National Monuments and Icons Sector

53. October 6, Porterville Recorder – (California) **Removal of illegal marijuana plot from park.** On September 29, law enforcement rangers removed an illegal marijuana grow, with a total of 13,077 plants (worth over $52 million), from the Sequoia National
Park, officials said in a news release. In addition, rangers found several hazardous materials that can cause harm to the natural environment at the site, including trash, fertilizers, pesticides, and herbicides, the release said. The plot is believed to have ties to a Mexican drug trafficking organization. No arrests have been made yet. The investigation is ongoing.


54. October 6, Associated Press – (Michigan) **Coast Guard investigates oil on Lake Huron beach.** U.S. Coast Guard investigators are trying to determine the source of an oil spill that soiled a Lake Huron beach at Cheboygan State Park in Cheboygan, Michigan. The spill was reported October 5, and cleanup crews were on the scene October 6. Oil covered a section of beach measuring about 25 yards by 300 yards. A sheen estimated at 5 yards by 300 yards was drifting offshore in Duncan Bay. A Coast Guard petty officer said the spill is not getting bigger. A tugboat and a car ferry are in the area, one anchored and the other aground. Investigators are planning to take samples from both to determine if the oil came from either. The Coast Guard said park rangers have closed affected sections of the beach for public safety.

Source: http://www.google.com/hostednews/ap/article/ALeqM5i8nA8cV-9CX6gKv_qrM5K4BrHeCwD9IMGO8G1?docId=D9IMGO8G1

[Dams Sector]

55. October 7, BBC News – (International) **Hungarian chemical sludge spill reaches Danube.** Toxic red sludge from a spill at an industrial plant in Hungary reached the River Danube October 7, officials said. They said alkaline levels that killed all fish in one river were greatly reduced, but were being monitored. Countries downstream from Hungary, including Croatia, Serbia and Romania, are drawing up emergency plans to protect against the mud, which burst out of a reservoir October 4. A million cubic meters spilled from a reservoir at an alumina plant in Ajka. Four people were killed and about 120 injured. The mud also caused massive damage in nearby villages and towns, as well as a wide swath of farmland. A disaster official said all life in the Marcal river, which feeds the Danube, had been “extinguished.” Tests are being carried out for two potential hazards — a powerful alkaline solution and heavy metals. Visiting the village of Kolontar, Hungary’s president said the worst-hit areas would have to be abandoned. Police have opened a criminal negligence inquiry into the incident. A BBC reporter witnessed bulldozers and trucks working through the night to reinforce a protective ring of earth below the industrial waste reservoirs, which are still intact. The reservoirs stretch in a line several kilometers below the aluminium factory. A Greenpeace spokesman called the spill “one of the top three environmental disasters in Europe in the last 20 or 30 years.”

Source: http://www.bbc.co.uk/news/world-europe-11491412

56. October 7, Associated Press – (International) **Sludge flood like Hungary’s unlikely in U.S.** Images like those from Hungary of homes surrounded by red mud and cars
floating through toxic sludge from a nearby metals plant would be unlikely in the United States, where only two states have similar facilities, according to industry officials and regulators. Texas and Louisiana are the only states with alumina factories like the one that malfunctioned in Europe, and they store the waste from the mining in a “dry” form, so even if a levee broke, the sludge could not become a threatening river, officials said. The levees that surround the storage beds also are designed to withstand winds from the most powerful hurricanes, and are periodically checked by state and federal regulators. In Ajka, Hungary, a reservoir that stored the red waste burst open October 4, rapidly becoming a devastating torrent of toxic mud, entering people’s homes, carrying away cars and killing at least four people. The sludge has already reached the Danube River — one of Europe’s main waterways. It is a byproduct of refining bauxite into alumina, the basic material for making aluminum. A spokesman for the Washington-based Aluminum Association said when people from the industry lobbying group first saw the images from Hungary, “it didn’t immediately make sense to us” because in the United States the material is dried before being stored. To have enough material to break a dam and flood a town “is pretty astonishing,” he added.

Source: http://www.google.com/hostednews/ap/article/ALeqM5hp2QEkrMMLRbL0QdnZZzB1UsBK8gD9IMTU8G0?docId=D9IMTU8G0

57. **October 6, Associated Press – (Iowa) Red Rock Dam gets much-needed service work.** Lots of dry days and a lake level draw-down mean much-needed maintenance work can now be done on the dam at Lake Red Rock in Marion County, Iowa, just north of Knoxville. When the lake is at its normal level, the access point for the cables that open and close the gates are under water. The Army Corps of Engineers threw open the spillway gates, draining an extra 10 feet off of the lake’s normal pool level. “The dam is a very well-made, well-designed machine. But it’s like any other 40-year-old machine, it needs maintenance,” a spokesman with the Army Corps of Engineers said. In this case, the maintenance involves the cables that lift the gates. They are scheduled to be replaced every 15 years. It was supposed to happen in 2008, but there have been too few many floods. The dam is being fixed, but it is going to take the Corps and the Iowa Department of Natural Resources (DNR) a lot longer to find a solution to lake red rock’s other problem: silt. The water policy director for DNR said, “We’re figuring that we’ve got over 400,000 dump truck loads of sediment coming in to this lake every single year.” The DNR is now working with cities and farmers to reduce runoff and stop the silt. If the sediment is not stopped, the fear is that it could someday fill the 15,000-acre lake.


58. **October 6, KERO 23 Bakersfield – (California) Isabella Dam Draft Environmental Assessment now available.** The draft environmental assessment (EA) for the Army Corps of Engineers’ Isabella Lake Auxiliary Dam Left Abutment Project is now available for public review and comment through Oct. 18, 2010. The project would raise the height of the auxiliary dam in California with a 200-foot earthen embankment, correcting a potentially dangerous low spot that could overtop in high water. The Auxiliary Dam Left Abutment Project is an interim measure to improve dam safety
until a more permanent solution to seepage and seismic issues at Isabella Dam under the Corps’ Isabella Lake Dam Safety Modification Project is put in place. The embankment and staging area for the project would be located on U.S. National Forest System land within the Sequoia National Forest. Soil for the embankment would come from the Kelso Creek Community Material Pit, under the jurisdiction of the U.S. Bureau of Land Management. Construction is scheduled to be completed by November 2010, before the start of the rainy season.


59. October 6, Thibodaux Daily Comet – (Louisiana) **South Lafourche levees fail corps inspection.** South Lafourche’s federal levee system in Louisiana failed an inspection by the Army Corps of Engineers, and Corps officials said use of poor-quality soil and steep slopes on some levees could put residents at risk of flooding. The local Levee District has until the beginning of November to come up with a plan to bring the Larose-to-Golden Meadow levee system into compliance. If it doesn’t, the levee will be dropped from the Corps’ rehabilitation and inspection program, and the Corps won’t pay to repair levees damaged by storms.


60. October 5, Associated Press – (Oregon) **Spillway gates concerns reduce Ore. dam storage.** Concerns about spillway gates atop 11 Willamette Valley dams near Salem, Oregon have prompted the U.S. Army Corps of Engineers to reduce water storage until the gates are repaired or replaced. The Statesman Journal reports the loss of storage capacity means the dams will be releasing more water during a longer period of time this winter and spring as a flood-control strategy. The entire network of dams holds back about one-fourth of the runoff each year in the Willamette River Basin. The Army said the project is estimated to cost about $150 million and will take years.


61. October 4, Wassau Daily Herald – (Wisconsin) **Statewide flood damage tops $10M.** Damage from late September rain and flooding has topped $10 million, according to a report October 4 from Wisconsin Emergency Management. The report shows reported damage to public infrastructure at $10,101,373. In addition, 441 homes and 58 businesses have reported minor damage, 33 homes and 10 businesses are reporting major damage and three homes, all in Marathon County, have been destroyed. The state does not calculate costs for residential and business damage. Wood County officials are reporting about $1.1 million in public sector costs, and Portage County is reporting about $570,000. The most recent report for Marathon County was issued October 1, and included a reported $201,000 in public sector damage. Buffalo, Clark, Columbia, Jackson, Marathon, Portage, Trempealeau, and Wood counties remained under a State of Emergency. Federal Emergency Management Agency officials are in state this week for damage assessments. Depending on damage estimates, an assessment may or may not take place in Marathon County. Additional damage
assessments may be released.

Source:
http://www.wausaudailyherald.com/article/20101004/WDH0101/101004129/Statewide-flood-damage-tops-10M

For another story, see item 26

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.