Department of Homeland Security Daily Open Source Infrastructure Report for 19 October 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- CNN reports authorities in Massachusetts evacuated thousands of residents as a wooden dam was failing, threatening to send up to six feet of water into the center of the southeastern town of Taunton. (See item 10)

- The Baltimore Sun reports authorities in Baltimore shut down portions of Interstate 95 for nearly two hours on Tuesday, October 18, and caused gridlock throughout the metropolitan region as police and federal agents investigated a threat to blow up either the Harbor or Fort McHenry tunnels. (See item 13)

- CNN reports an additional 12 birds have tested positive in Romania for the deadly strain of bird flu, and officials have vaccinated 100,000 Romanians against common strains of influenza in an attempt to limit the possibility the virus might gain the ability to spread easily from person to person. (See item 20)

- The US−CERT has released "Technical Cyber Security Alert TA05−291A: Snort Back Orifice preprocessor buffer overflow." (See item 30)

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 18, Tampa Bay 10 (FL)* — **Power substation shot at in Florida.** Sometime on Friday, October 14, or Saturday, October 15, a Progress Energy power substation near Bartow, FL was shot with five rounds from a high−powered rifle. An oil tank was ruptured, causing more than $600,000 in damages. According to the Polk County Sheriff’s Office, the oil tank leaked all night, and an explosion occurred, leaving customers without power for several hours.
Source: http://www.tampabays10.com/news/news.aspx?storyid=20070

2. *October 18, The Arizona Republic* — **Nuclear plant emergency system deemed safe, plant to resume operations.** The Palo Verde Nuclear Generation Station, just west of Phoenix, AZ, will go online again by the end of the week. On Monday, October 17, two of the three reactors began preparations to resume operations. The two units, which generate approximately 2,600 megawatts, were shut down after Arizona Public Service (APS) could not prove to the Nuclear Regulatory Commission that the system’s emergency cooling system would function properly during an emergency. Jim Levine, an executive vice president for APS, said, "The decision to take the units off line was the right one and demonstrates our full commitment to safe operation.” He said that the latest analysis confirms the system would flood a reactor with water in the event of a loss−of−coolant accident.
Source: http://www.azcentral.com/arizonarepublic/local/articles/1018 aps18.html

3. *October 17, Department of Energy* — **Department of Energy funds projects designed to boost recovery of unconventional resources.** Department of Energy (DOE) Secretary Samuel Bodman says that DOE will provide $10.7 million to fund 13 research and development projects that focus on recovering large, unconventional gas and oil resources. Additional support from industry and academic partners will boost the total value of investment to $16.3 million. According to DOE, most of the research projects will increase the recovery of unconventional natural gas, which can be found in coal seams, low−permeability or “tight” sandstones, and ultra−deep natural gas resources found more than 15,000 feet underground. Currently, unconventional natural gas accounts for almost one quarter of total domestic supply, and this is expected to increase with technological advances. Other projects funded include “smart” drilling systems that will withstand the extreme temperatures, pressures, and corrosive conditions of deep reservoirs.
Source: http://www.energy.gov/engine/content.do?PUBLIC_ID=18982&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE

4. *October 16, Gulf News (UAE)* — **Qatar plans to increase amounts of liquefied natural gas it exports to U.S.** Qatar Liquefied Gas Co (Qatargas) and Ras Laffan Qatar Liquefied Gas Co (RasGas), have reached heads of agreements (HoAs) with ExxonMobil, ConocoPhillips, Florida Power and Light Group, and international companies as part of an overall production package that will increase Qatar’s production capacity to about 77 million tons per annum (mtpa) in 2012. Of this, nearly 30 mtpa is planned to reach the U.S. if the HoAs are converted into purchase agreements. Qatar plans to spend a $15 billion to add 70 vessels to its fleet of tankers to export LNG. If the pace of expansion continues, Qatar could overtake Indonesia as the largest supplier of LNG in the world as early as 2007.
Source: http://www.gulf−news.com/Articles/OpinionNF.asp?ArticleID=18 7002

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *October 18, WQAD (IL)* — **Iowa interstate spill prompts lane closure.** Davenport, IA, Hazmat crews spent much of Monday night, October 17, cleaning up a hazardous chemical leak on Interstate 80 near the Stockton exit. A semi−truck driver in the westbound lane of traffic crossed over into the east bound lane and into a field. Hazmat crews say the truck spilled some hazardous chemicals. The driver was taken to the hospital and treated for non−life−threatening injuries. Only one vehicle was involved. No word on what the chemicals were, or if they presented any kind of danger. One lane of the interstate was closed in the eastbound direction.
Source: http://www.wqad.com/Global/story.asp?S=3991927&nav=1sW7Doua

6. *October 17, Middletown Journal (OH)* — **Tanker overturns in Ohio, leaking liquid nitrogen and prompting road closure.** A semi−truck carrying liquid nitrogen flipped over on Todhunter Road in Monroe, OH, just after 12 p.m. EDT Sunday, October 16, and spilled liquid nitrogen in the area of North Main Street and Todhunter Road. An Air Liquide Industrial semi−truck traveling south on North Main Street overturned and slid for 300 feet on its side after swerving to miss an oncoming vehicle traveling on Todhunter Road, said Monroe police officer Gregg Miers. The oncoming vehicle, according to witnesses, pulled out from Todhunter Road into the truck's path, then kept going as the truck swerved to avoid colliding with the vehicle. The truck driver was transported to Middletown Regional Hospital with minor injuries, Miers said. No other injures were reported. When released in an open environment, liquid nitrogen evaporates into the atmosphere quickly and is no longer dangerous, Miers said. The road was shut down for several hours; however, there were no evacuations. Police are still investigating the incident and looking for the second vehicle, which did not stop at the scene of the accident.
Source: http://www.middletownjournal.com/news/content/news/stories/2005/10/17/mj1017spill.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.

[Return to top]

Banking and Finance Sector

7. *October 18, Silicon.com* — **Crime bosses plot smarter fraud attacks on banks.** Banks have been warned to prepare for a new wave of more sophisticated fraud attacks from organized criminals. Scammers will start developing more sophisticated attacks as they move on from simple phishing frauds, according to John Meakin, group head of information security at Standard Chartered Bank. Speaking at the Financial Services IT Summit in London he said: "We don't have a monopoly on the security expertise −− the thing about organized crime is that they have the money and the leverage. They pick off the easy stuff first and that means soft

targets and simple mechanisms −− and you can't get more simple than phishing." While banks are too difficult a target at the moment he added: "Looking into the future there is no question that in five years time they will be looking to keep up that revenue stream which means more sophisticated targets and technologies." Meakin warned that one area of threat is continuing vulnerabilities in browser technologies which make 'man−in−the−middle' attacks possible. This is where an attacker can interfere with the communications between the browser and a Website to their own ends.
Financial Services IT Summit: http://www.cnetnetworks.co.uk/etf/fs−itsummit/index.html
Source: http://www.silicon.com/financialservices/0,3800010364,391534 30,00.htm

8. *October 17, WISH TV (IN)* — **University center fights online crime through research.** Indiana University’s Center of Applied Cybersecurity Research is studying ways to combat online scams such as phishing. “We are devising better attacks. Second, we are asking why was this attack successful; why did our attack succeed? Then we develop counter measures,” says Markus Jakobsson, assistant director of the Center. Jakobsson says if a potential thief can figure out what bank consumers use or which Websites are visited, that consumer could be an easy target for a phishing scam. The researchers design programs that search browsers for the online bank used, and just from a name and date of birth of a person in Florida, one of their programs can get their driver’s license number. Those programs replicate what criminals can do. They have helped companies like eBay shutdown phishing schemes.
Indiana University Center of Applied Cybersecurity Research: http://cacr.iu.edu/
Source: http://www.wishtv.com/Global/story.asp?S=3991164&nav=0Ra7

9. *October 17, IT Observer* — **Cardholder not present fraud increasing.** Of the security issues facing banks, prevention of card fraud is set to grow even further in importance. The level of card fraud has risen significantly over recent years, caused primarily by the explosion in the number and usage of payment cards and the associated high level of organized card crime activity. As new banking channels have opened, for example Internet, phone banking and e−commerce, and the boom in credit card use, crime has migrated to seek any opportunity to attack these new and immature transaction methods. The losses associated with these attacks have risen drastically over the past couple of years, and the most costly type of card fraud is that of Cardholder−Not−Present (CNP) fraud. CNP transactions are performed remotely, when neither the card nor the cardholder is present at the point−of−sale. In CNP transactions, retailers are unable to physically check the card or the identity of the cardholder, which makes the user anonymous and able to disguise their true identity. Fraudulently obtained card details are generally used with fabricated personal details to make fraudulent CNP purchases. The card details are normally copied without the cardholder’s knowledge, taken from discarded receipts or obtained by skimming.
Source: http://www.ebcvg.com/articles.php?id=940

[Return to top]

Transportation and Border Security Sector

10. *October 18, CNN* — **Massachusetts dam threatens to flood town.** Authorities in Massachusetts evacuated thousands of residents as a wooden dam was failing, threatening to send up to six feet of water into the center of the southeastern town of Taunton. A second dam

up the Mill River also could be threatened if the structure, known as the Dam at Whittenton Mills, fails, Governor Mitt Romney said. Torrential rain last week and overnight have swollen the river and deteriorated the 12−foot Dam at Whittenton Mills, said Mayor Robert Nunes, threatening the town of 56,000, about 30 miles south of Boston Nunes declared a state of emergency Monday evening, October 17. About 2,000 people in low−lying areas and in the downtown area have been evacuated, including a housing development for the elderly, authorities said. By midday Monday, the dam's railing was dipping, and some of its pilings were beginning to show signs of failure, officials said. If the Whittenton dam goes, then the second dam −− the Morey's Bridge Dam about a half−mile away −− might burst, sending as much as 12 feet of water through the area, Romney said.
Source: http://www.cnn.com/2005/US/10/18/massachusetts.dam/index.htm l

11. *October 18, Associated Press* — **FAA investigates near−misses at Boston's Logan.** A team of specialists from the Federal Aviation Administration (FAA) toured Logan International Airport on Monday, October 17, to investigate a rash of near−collisions on its runways. Members of the FAA's "Tiger Team" will spend two or three days studying Logan's runway safety procedures and evaluating the performance of its air−traffic controllers, according to FAA spokesperson Jim Peters. "It's not just the controllers we're looking at," Peters said. "We're looking at everything because some of the (near−collisions) have been attributed to actions taken by pilots." Logan has had 16 "runway incursions" since last October, including an incident earlier this month in which a jet had to abort its takeoff when it crossed paths with another jet on the runway. The fact that Logan has five cramped, intersecting runways may explain why there have been more incursions there than at other airports of its size. Once the team completes its evaluation, it will issue its findings in a report to FAA chief Marian Blakey. Two members of the "Tiger Team" at Logan this week are Massachusetts Port Authority employees. "They bring with them a vast amount of knowledge on how the airport operates," Peters said. "It's to our benefit to include them on the team."
Source: http://www.thebostonchannel.com/news/5114940/detail.html

12. *October 18, Government Computer News* — **FAA behind on IT security reforms, IG finds.** The Federal Aviation Administration (FAA) has fallen short of its goals to complete security reviews of its air traffic control systems, according to a recent report by the Department of Transportation's inspector general. In the report, the IG concluded that the FAA took only limited steps to perform security reviews at all air traffic locations, despite stating last year that the agency would complete the reviews within three years. "FAA collected system security information on only about half of the systems used to support en−route [high−altitude] air traffic systems," the report said. "En−route centers currently rely on approximately 30 systems to deliver safe and efficient air traffic control services. Since information was collected only on half of the systems, other critical systems, such as the system that routes critical weather and flight plan data to all en−route centers, were not reviewed." The Department of Transportation, the report said, must strengthen its security management so weaknesses are fixed in a timely manner. Transportation officials in response said they agreed with the IG's conclusions and would outline steps to be taken for improvement.
Report: http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/DOT_FIS MA.pdf
Source: http://www.gcn.com/vol1_no1/daily−updates/37318−1.html

13.

October 18, Baltimore Sun — **Threat briefly shuts portions of I−95 in Baltimore.** Authorities in Baltimore shut down portions of Interstate 95 for nearly two hours on Tuesday, October 18, and caused gridlock throughout the metropolitan region as police and federal agents investigated a threat to blow up either the Harbor or Fort McHenry tunnels. The closures began about 11:30 a.m. EDT and officers began reopening the tubes about 1:15 p.m. Federal law enforcement officials said the threat was made against an unspecified tunnel by an informant in a foreign country who said a suspect was a man of Egyptian origin living in the Baltimore area. The informant's information was uncorroborated, the official said. The investigation has been ongoing for the past two or three days, but the decision to close the tunnels was made by the Maryland Transportation Authority Police, who apparently were concerned that the suspects may act as word of the investigation got out. "Acting out of an abundance of caution [the Maryland Transportation Authority Police] elected late this morning to close the Harbor Tunnel in both directions and to allow only limited access at the Fort McHenry tunnel," said Jim Pettit, a spokesperson for the Maryland Department of Transportation. The area most immediately affected was I−95 near the tunnels and Key Highway, which is also near the Maryland Port.
Source: http://www.baltimoresun.com/news/custom/attack/bal−tunnel1018,1,510663.story?coll=bal−home−headlines&ctrack=1&cset=true

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

14. *October 18, Salt Lake Tribune (UT)* — **Two more deer found with chronic wasting disease.** Utah wildlife officials on Monday, October 17, confirmed two more cases of chronic wasting disease (CWD) in buck mule deer killed by hunters. The known total of cases of deer with the fatal nervous system disease in Utah now stands at 20. The two new cases were in animals killed during the state muzzleloader season in late September and early October. A mature buck taken on the LaSal Mountains east of Moab pushes the number of CWD cases in that area to 14. The LaSals are a hot spot for CWD in Utah, but biologists believe only two percent of the animals in that area have the disease. The other animal, a yearling buck, was killed near the south end of Flaming Gorge Reservoir, about 20 miles north of the site where four other deer tested positive for the disease. The only other case of CWD came from the Fountain Green area in 2003. "We've tested approximately 450 deer and elk so far this year, and these are the only animals that have tested positive for CWD," Leslie McFarlane, wildlife disease specialist for the Division of Wildlife Resources said.
Source: http://www.sltrib.com/utah/ci_3127023

15. *October 17, Agence France Presse* — **Brazil confirms three new foot−and−mouth cases.** Top beef exporter Brazil confirmed three new foot−and−mouth outbreaks in southwestern cattle farms, one week after the first case prompted Brazilian beef import bans in more than 30

countries. The new cases were found in three farms in Mato Grosso do Sul, where the first outbreak was discovered October 10, according to the agriculture ministry. One of the properties is located in Eldorado, where the first foot−and−mouth case was found. The two other incidents were found in nearby Japora, according to an agriculture ministry spokesperson. The Eldorado farm has more than 3,500 cattle, but officials had no figures for the two other farms. The first outbreak occurred in a herd of 582 cows, which were destroyed. Foot−and−mouth disease is a highly contagious illness that affects cows, sheep, pigs, and horses. Brazil became the world's largest beef exporter last year and has one of the largest herds in the world, with 195 million cattle.
Source: http://news.yahoo.com/s/afp/20051017/hl_afp/brazilfarmhealth beef_051017233345;_ylt=AqpW3hxVEnJAnla3VANLpkGJOrgF;_ylu=X3o DMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Food Sector

16. *October 18, New York State Department of Agriculture & Markets* — **Tuna salad recalled.** Home Made Brand Foods Inc., of Newburyport, MA, is recalling Classic Tuna Salad, due to Listeria contamination. Listeria is a common organism found in nature. It can cause serious complications for pregnant women, such as stillbirth. Other problems can manifest in people with compromised immune systems. Listeria can also cause serious flu−like symptoms in healthy individuals. The problem was discovered after routine sampling by New York State Department of Agriculture and Markets Food Inspectors and subsequent analysis of the product by Food Laboratory personnel found the product to be positive for Listeria monocytogenes.
Source: http://www.agmkt.state.ny.us/AD/alert.asp?ReleaseID=647

17. *October 18, Korea Herald* — **Decision on U.S. beef imports due in October.** South Korea will decide between the end of this month and early November whether to resume U.S. beef imports now that Seoul has received its requested information, a government official said Monday, October 17. "The livestock quarantine panel is expected to meet around the end of this month or early November after it has examined all the information related to mad cow cases that Seoul requested from Washington," said Kim Chang−seob, director of the Animal Health Division, Livestock Bureau at the Ministry of Agriculture and Forestry. Korea banned U.S. beef imports in December 2003 when a case of the brain−wasting illness bovine spongiform encephalopathy was discovered on a Washington state cattle farm. Then a second confirmed case this June further delayed Seoul's plan to decide whether to reopen its borders. The panel, expected to convene soon, is comprised of both government and civilian experts. They will be examining the latest steps taken by the U.S. government to ensure that the beef is safe to consume. In 2003, Korea was the third−largest importer of U.S. beef.
Source: http://www.koreaherald.co.kr/SITE/data/html_dir/2005/10/19/2 00510190016.asp

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

18. *October 18, Bloomberg* — **Indonesia polio cases rise as disease spreads to Aceh.** Indonesia's cases of polio rose to 269 from 240 three weeks ago as the disease spread to the tsunami−devastated province of Aceh on Sumatra Island, an official at the World Health Organization (WHO) said Tuesday, October 18. In the past two weeks, new cases were also found in Riau province in east Sumatra, and in Palembang city in the south, Thomas Moran, a WHO spokesperson, said in a phone interview. "It is worrying that polio is spreading quickly in Sumatra," he said. "It shows there are still pockets of un− immunized children." Two rounds of a nationwide vaccination program have been successful in reducing the rate of increase of the disease, which mostly affects children under five years old, in the nation's first polio outbreak in a decade, Moran said. About 1,354 cases of polio have been confirmed in 16 countries this year, WHO said. The spread of polio, which causes paralysis and sometimes death, in countries like Nigeria, is delaying efforts to globally eradicate the virus by at least a year, the WHO said on October 13.
Global polio eradication initiative: http://www.polioeradication.org/
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=a2V87kAv0fxU&refer=asia

19. *October 18, Associated Press* — **Farm worker's death traced to hantavirus.** The death of a farm worker in Grant, WA, last month has been traced to hantavirus, health officials said. The count health department's personal health services director, Peggy Grigg, said authorities were providing hantavirus prevention information to businesses and residents in the area. Laboratory tests this month showed the worker died of the disease, which is spread by exposure to the dried feces and urine of rodents, mostly deer mice. The disease was virtually unknown in the U.S. before an outbreak in 1993 in the Four Corners area of Utah, Colorado, New Mexico, and Arizona. Since then, Washington has had 27 reported cases, nine of them fatal.
Hantavirus information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://seattlepi.nwsource.com/local/244971_guard18.html

20. *October 18, CNN* — **Twelve new bird flu cases reported in Romania.** An additional 12 birds have tested positive in Romania for the deadly strain of bird flu that has already killed at least 60 people in Asia, Minister of Agriculture Ghearghe Flutur said Tuesday, October 18. The H5N1 strain of the virus was found in a dozen dead swans near the Ukrainian border. Earlier Romania cases were discovered in the counties of Tuleca and Constanza, near the Black Sea. In the villages of Ceamurlia and Maliuc, in Tuleca County, almost 60 birds have died from avian flu, authorities said. Live birds are no longer available for sale in markets, and approval from a veterinarian is needed to sell even slaughtered chickens. Officials said they had vaccinated 100,000 Romanians against garden−variety strains of influenza in an attempt to limit the possibility that the virus that causes bird flu might, through "reassortment" with the more common form, gain the ability to spread easily from person to person.
Source: http://edition.cnn.com/2005/HEALTH/conditions/10/18/birdflu. romania.tues/

21.

October 18, Associated Press — **Anthrax and drug−resistant TB storage unregulated at almost 60 labs in Japan.** Almost 60 medical and research facilities in Japan own samples of bacteria that could be used in bioterrorism, but have no guidelines on how the dangerous agents should be stored, a government report has said. At least 79 labs across Japan said they keep samples of multi−drug resistant tuberculosis (MDR TB), while 27 facilities had the anthrax agent and a further eight possessed samples of both, according to a survey released earlier this month by Japan's Health, Labor and Welfare Ministry. Of these, over half, or 58 facilities, used no manual on handling or storing the potentially lethal microbes, the study said. MDR TB and anthrax, both potentially highly lethal, can be easily spread from person to person. Experts have said the agents could easily be engineered for terrorist attacks.
Source: http://mdn.mainichi−msn.co.jp/national/news/20051018p2a00m0n a018000c.html

22. *October 17, Reuters* — **Chiron warns of flu vaccine shortfall.** Chiron Corp. on Monday, October 17, said its U.S. flu vaccine deliveries will fall short this year due to production problems at its British manufacturing plant. Chief Executive Howard Pien, speaking on a conference call, said the plant would produce fewer than 18 million doses for the 2005 to 2006 flu season, down from the company's previous estimate of 18 million to 26 million doses. Chiron's plant in Liverpool, England was recently restarted after being shut down due to contamination problems a year ago. That abrupt shutdown cut the U.S. vaccine supply in half. Despite Chiron's lowered projections, the U.S. Food and Drug Administration said it expected there would be significantly more vaccine produced than last year. Chiron attributed this year's shortfall to delays related to changes at the plant as well as lower output associated with adapting new processes and procedures.
Source: http://www.nytimes.com/reuters/business/business−chiron.html

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

23. *October 18, Contra Costa Times (CA)* — **California Bay Area unites for disaster response plans.** The mayors of Bay Area, CA's, three largest cities on Monday, October 17, announced a new initiative to bring regional coordination to the emergency response plans that communities develop to prepare for large−scale disasters. The mayors of San Francisco, Oakland and San Jose gathered at the Cypress Freeway Memorial Park to announce a two−year, $2.2 million effort to maximize the Bay Area's emergency resources. Oakland Mayor Jerry Brown, San Francisco Mayor Gavin Newsom and San Jose Mayor Ron Gonzalez called the effort the first of its kind in the U.S. It is being spearheaded by San Francisco, which is providing federal Homeland Security funds to pay the lion's share of the planning effort. The first phase of the project will be to inventory the emergency assets available within the ten counties participating in the project. Those counties include the nine Bay Area counties plus Santa Cruz. The next phase will be to develop clear guidelines for how those assets should be used in a major

disaster. First responders within the ten counties will then take part in a series of workshops, seminars and multi−jurisdictional exercises to test components of the plan before it is finalized.
Source: http://www.contracostatimes.com/mld/cctimes/12931001.htm

24. *October 18, Morning Sentinel (ME)* — **Maine State Police Chief: Communications key when disaster strikes.** Maine State Police Chief Colonel Craig Poulin on Monday, October 17, described the state's 30−year−old radio communications system as a highway with potholes and crumbling bridges. It's "falling apart" and has had major failures, he said. Updating the state's communications system will be the key to being prepared in a disaster, he told members of the Task Force to Study Maine's Homeland Security Needs, which kicked off Monday, October 17. The upgrade, which will be done in phases over five years, is scheduled to get $20 million in state funding, said Shawn Romanoski, the state's communication coordinator. When complete, the system will serve as a much improved highway for communication among emergency responders, but it will be up to local cities and towns to buy compatible equipment, Poulin said. At its first meeting, the 11−member task force heard from emergency management officials, police, fire, marine patrol and the Bureau of Health in an effort to learn more about whether the state is prepared to handle disaster. State officials emphasized that while Maine might not be at serious risk for a terrorist attack, emergency management personnel need to be able to respond to a whole host of disasters.
Source: http://morningsentinel.mainetoday.com/news/local/2062353.sht ml

25. *October 18, Aspen Times (CO)* — **Colorado county safety officials: Emergency response coordination is very advanced.** At a press conference Monday, October 17, in the Pitkin County, CO, Courthouse, officials from a variety of agencies said they are well ahead of the South, and most of the rest of the nation, in preparing for the unthinkable. The emphasis on local preparedness revolves around the council's incident command system, a management mode and organizational chart that allows officials to handle disasters effectively. Joe DiSalvo, chief of investigations for the sheriff's office, said the system is used for everything from car accidents to presidential visits. Pivotal in the system is communication: Everyone knows their roles and responsibilities, which Aspen Police Chief Loren Ryerson said helps eliminate arguments over authority. The top positions on the organizational chart, such as incident commander, are interchangeable. This means that in a large wildfire, for instance, a sheriff's official could run the logistics side of things to free up firefighters for their main task. Within the incident command system are more plans, including ones that cover radio frequencies, medical plans and weather reports. "Whatever life throws at us, we'll be able to handle it," said Ellen Anderson, Pitkin County emergency management coordinator.
Source: http://www.aspentimes.com/article/20051018/NEWS/110180018

26. *October 18, Government Accountability Office* — **GAO−06−119: Federal Emergency Management Agency: Improvements Needed to Enhance Oversight and Management of the National Flood Insurance Program (Report).** In the wake of Hurricane Isabel in 2003, the Government Accountability Office (GAO) was mandated by the Flood Insurance Reform Act of 2004 to report on issues related to the National Flood Insurance Program (NFIP) and its oversight and management by the Federal Emergency Management Agency (FEMA). Private insurance companies sell NFIP policies and adjust claims, while a private program contractor helps FEMA administer the NFIP. To address this mandate, this report assesses (1) the statutory and regulatory limitations on coverage for homeowners under the NFIP, (2) FEMA's role in

monitoring and overseeing the NFIP, (3) FEMA’s response to concerns regarding NFIP payments for Hurricane Isabel claims, and (4) the status of FEMA’s implementation of provisions of the Flood Insurance Reform Act of 2004. Although impacts from Hurricane Katrina were not part of the report’s scope, GAO recognizes that this disaster presents the NFIP with unprecedented challenges. GAO is recommending that FEMA use a statistically valid method to select claims for review and establish milestones for meeting provisions of the Flood Insurance Reform Act. FEMA reviewed a draft of this report and expressed concerns about GAO's findings related to NFIP program management.
Highlights: http://www.gao.gov/highlights/d06119high.pdf
Source: http://www.gao.gov/new.items/d06119.pdf

27. *October 18, Government Accountability Office* — **GAO−06−174T: Federal Emergency Management Agency: Challenges Facing the National Flood Insurance Program (Testimony).** The disastrous hurricanes that have struck the Gulf Coast and Eastern seaboard in recent years −− including Katrina, Rita, Ivan, and Isabel −− have focused attention on federal flood management efforts. The National Flood Insurance Program (NFIP), established in 1968, provides property owners with some insurance coverage for flood damage. The Federal Emergency Management Agency (FEMA) within the Department of Homeland Security is responsible for managing the NFIP. This testimony offers information from past Government Accountability Office (GAO) work on (1) the financial structure of the NFIP, (2) why the NFIP insures properties for repetitive flood losses and the impact on NFIP resources, and (3) compliance with requirements for mandatory purchase of NFIP policies. The testimony also discusses recommendations from a report GAO issued Tuesday, October 18, on FEMA’s oversight and management of the NFIP. In the report released Tuesday, GAO is recommending, among other things, that FEMA and its partners use a statistically valid approach to sample NFIP insurance claim files for quality assurance purposes, and that DHS and FEMA develop and document plans for implementing requirements of the Flood Insurance Reform Act of 2004, which reauthorized the NFIP. FEMA disagreed with those recommendations.
Highlights: http://www.gao.gov/highlights/d06174thigh.pdf
Source: http://www.gao.gov/new.items/d06174t.pdf

28. *October 18, Associated Press* — **Phone service, 911 knocked out in Southern California.** An equipment problem knocked out long−distance telephone service and parts of the 911 system for tens of thousands of residential and business customers in several Southern California cities Tuesday, October 18, officials said. The problem began around 2:20 a.m. PDT at Verizon Communications Inc.'s central office in Long Beach, CA, Verizon spokesperson Bill Kula said. Service was out in cities including Long Beach, Huntington Beach, Laguna Beach, Artesia, Downey, Bellflower and Westminster, he said. Local calls were possible but long distance service was interrupted. He said he did not immediately know what caused the problem or how many customers were affected. Long Beach activated its emergency operations center, and fire and police departments increased patrols to watch for problems, said Jeff Reeb, a spokesperson for the Long Beach Fire Department. Reeb said he was unaware of any significant emergency response issues. People could reach emergency dispatchers by dialing 911 on cell phones or calling an alternate number. Emergency service also was unavailable in several Los Angeles County beach communities to the north, Hermosa Beach police Sergeant Paul Wolcott said. Kula said he did not know if those problems were related to the equipment failure in Long Beach.

Source: http://www.breitbart.com/news/2005/10/18/D8DAHOJG1.html

29. *October 17, Richmond (VA)* — **Virginia Governor Mark R. Warner dedicates police and emergency headquarters.** Virginia Governor Mark R. Warner on Friday, October 14, officially dedicated Virginia's Combined State Police Headquarters and Emergency Operations Center in Chesterfield County, VA. Built at the existing Virginia State Police administrative headquarters, the $15 million addition will house the administrative offices of Virginia State Police, the new Virginia Fusion Center, and the new state−of–the−art Virginia Emergency Operations Center (EOC). The new Virginia EOC is six−times larger than the current 2,500 square foot facility housed in a Cold War−era space underneath the Virginia State Police Academy. The new EOC, under the direction of the Virginia Department of Emergency Management, is scheduled to become operational by the year's end. "The current EOC was crowded, difficult to access, and seriously outdated. Cell phones and Blackberries don't work underground in the old EOC bunker –− which is supposed to be our communications hub in a disaster. This new facility with the latest technology and a centralized work area will improve communication and teamwork, and ultimately will save lives," said Warner.
Source: http://www.richmond.com/news/output.aspx?Article_ID=3941283&Vertical_ID=23&tier=10&position=1

[Return to top]

Information Technology and Telecommunications Sector

30. *October 18, US−CERT* — **Technical Cyber Security Alert TA05−291A: Snort Back Orifice preprocessor buffer overflow.** Snort preprocessors are modular plugins that extend functionality by operating on packets before the detection engine is run. The Back Orifice preprocessor decodes packets to determine if they contain Back Orifice ping messages. The ping detection code does not adequately limit the amount of data that is read from the packet into a fixed−length buffer, thus creating the potential for a buffer overflow. The vulnerable code will process any UDP packet that is not destined to or sourced from the default Back Orifice port (31337/udp). An attacker could exploit this vulnerability by sending a specially crafted UDP packet to a host or network monitored by Snort. A remote attacker who can send UDP packets to a Snort sensor may be able to execute arbitrary code. Snort typically runs with root or SYSTEM privileges, so an attacker could take complete control of a vulnerable system. An attacker does not need to target a Snort sensor directly; the attacker can target any host or network monitored by Snort.
Sourcefire has released Snort 2.4.3: http://www.snort.org/dl/
Additional information is available in US−CERT Vulnerability Note VU#175500:
http://www.kb.cert.org/vuls/id/177500
Source: http://www.us−cert.gov/cas/techalerts/TA05−291A.html

31. *October 17, Security Focus* — **Lynx NNTP article header buffer overflow vulnerability.** Lynx is prone to a buffer overflow when handling NNTP article headers. This issue may be exploited when the browser handles NNTP content, such as through 'news:' or 'nntp:' URIs. Exploitation may result in code execution in the context of the program user.
Source: http://www.securityfocus.com/bid/15117/references

32. *October 17, Computer World* — **Teen uses worm to boost ratings on MySpace.com.** Using a self−propagating worm that exploits a scripting vulnerability common to most dynamic Websites, a Los Angeles teenager made himself the most popular member of community Website MySpace.com earlier this month. While the attack caused little damage, the technique could be used to destroy Web site data or steal private information−−even from enterprise users behind protected networks, according to Jeremiah Grossman, chief technical officer at Santa Clara, Calif.−based WhiteHat Security Inc. The 19−year−old, who used the name "Samy," put a small bit of code in his user profile on MySpace, a 32−million−member site, most of whom are under age 30. Whenever Samy's profile was viewed, the code was executed in the background, adding Samy to the viewer's list of friends and writing at the bottom of their profile, "... and Samy is my hero." The worm spread by copying itself into each user's profile. Because of MySpace's popularity, the worm spread quickly. The attack depended on a long−known but little−protected vulnerability called cross−site scripting (XSS). XSS arises because many Websites−−apart from static sites that use only simple HTML code−−are dynamic, allowing users to manipulate Website source code.
Source: http://www.computerworld.com/securitytopics/security/story/0,10801,105484,00.html?SKC=security−105484

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports that Microsoft has released updates that address critical vulnerabilities in Windows, Internet Explorer, and Exchange Server. Exploitation of these vulnerabilities may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges or with the privileges of the user. If the user is logged on with administrative privileges, the attacker could take complete control of an affected system. An attacker may also be able to cause a denial of service.

Microsoft Security Bulletins for October 2005 address vulnerabilities in Windows and Internet Explorer. Further information is available in the following US−CERT Vulnerability Notes:

VU#214572 − Microsoft Plug and Play fails to properly validate user supplied data
VU#883460 − Microsoft Collaboration Data Objects buffer overflow
VU#922708 − Microsoft Windows Shell fails to handle shortcut files properly
VU#995220 − Microsoft DirectShow buffer overflow
VU#180868 − Microsoft Distributed Transaction Coordinator vulnerable to buffer overflow via specially crafted network message
VU#950516 − Microsoft COM+ contains a memory management flaw
VU#959049 − Several COM objects cause memory corruption in Microsoft Internet Explorer

VU#680526 − Microsoft Internet Explorer allows non−ActiveX COM objects to be instantiated

Microsoft has provided the updates for these vulnerabilities in the Security Bulletins and on the Microsoft Update site. For more information please visit URL: http://www.microsoft.com/technet/security/bulletin/ms05−oct. mspx

Top Source Port / IP Addresses: Increased reported port activity: 1026 UDP, 1026 UDP, 1029 UDP, 1030 UPD from the following IP blocks, located in China: 221.10.254.31,218. 66.104.208, 222.77.185.242, 221.27.16.180, 61.152.158.126, 221.6.77.72, 202.99.172.160, and 218.66.104.206

US−CERT strongly recommends that all users reference the Federal Emergency Management Agency (FEMA) web site for a list of legitimate charities to donate to their charity of choice. http://www.fema.gov/

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 26777 (−−−), 135 (epmap), 139 (netbios−ssn), 25 (smtp), 1025 (win−rpc), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

33. *October 18, Government Accountability Office* — **GAO−06−180T: Capitol Visitor Center: Status of Schedule, Fire Protection, Cost, and Related Issues. (Testimony).** The Government Accountability Office (GAO) is assisting the Subcommittee in monitoring progress on the Capitol Visitor Center (CVC) project. GAO's remarks will focus on (1) the Architect of the Capitol's (AOC) progress in managing the project's schedule since the Subcommittee's September 15 hearing on the project, (2) issues associated with the CVC's fire protection system, and (3) the project's costs and funding. The GAO remarks on Tuesday, October 18, are based on the review of schedules and financial reports for the CVC project and related records maintained by AOC and its construction management contractor; observations on the progress of work at the CVC construction site; and discussions with CVC project staff, AOC's Chief Fire Marshal, United States Capitol Police representatives, and officials responsible for managing the Capitol Power Plant. GAO did not perform an audit; but rather performed work to assist Congress in conducting its oversight activities. In summary, AOC and its construction contractors have made progress in managing the schedule and accomplishing work since the Subcommittee's September 15 CVC hearing, but additional delays have been encountered.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−180T

[Return to top]

General Sector

34. *October 18, George Mason University* — **Group meets to discuss security cost recovery programs for critical infrastructure investments in the National Capital Region.** The Senior Policy Group (SPG) of the Office of the National Capital Region Coordination and George Mason University's Critical Infrastructure Protection Program held the first Security Cost Recovery Workshop on Thursday, October 6, 2005, to discuss possible initial steps in the development of a single, harmonized legislative and regulatory program to encourage capital and operational expenditures in security in the National Capital Region. Workshop participants discussed the recovery of security costs incurred by regulated utilities, including water, electric, and telephone. The workshop was a result of recommendations that evolved from the National Capital Region−Critical Infrastructure Project (NCR−CIP). In 2002, the National Capital Region's Eight Commitments to Action identified critical infrastructure protection (CIP) as a high priority of homeland security strategy and required that the public and private sectors partner to identify and set protection priorities and guidelines for infrastructure assets and services in the NCR. The NCR Urban Area Homeland Security Strategy set strategic objectives to reduce the NCR's vulnerability to terrorism and minimize the damage and recover from attacks that do occur −− both critical infrastructure protection (CIP) objectives. With this focus, the SPG of the NCR directed an initiative to support regional CIP.
National Capital Region Project: http://cipp.gmu.edu/ncrproject/index.html
Source: http://cipp.gmu.edu/news/CRW_100605.html

35. *October 15, Federal Bureau of Investigation* — **Man arrested for alleged nuclear security hoax.** Jose Ernesto Beltran Quinonez was arrested in San Diego for perpetrating a terrorist hoax and making false statements concerning an alleged plot to smuggle a nuclear warhead into the United States from Mexico. On January 17, 2005, Beltran−Quinonez made a series of 911 calls from his cellular telephone wherein he alleged that a nuclear warhead was going to be smuggled into the United States within the next four days through a tunnel connecting Mexicali, Mexico, with Calexico, CA. The indictment further alleges that Beltran−Quinonez told the 911 operator that the warhead was to be delivered to a group of previously smuggled Iraqi and Chinese nationals, who were planning to transport the warhead to Boston.
Source: http://sandiego.fbi.gov/pressrel/2005/sd101505.htm

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

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.