Homeland Security

Daily Open Source Infrastructure Report for 27 November 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- According to the Associated Press, Toyota Motor Corp. said on November 25 it will replace accelerator pedals on 3.8 million recalled vehicles in the United States to address problems with the pedals becoming jammed in the floor mat. As a temporary step, Toyota will have dealers shorten the length of the gas pedals beginning in January while the company develops replacement pedals for their vehicles, the Transportation Department and Toyota said. (See item **8**)
- The IDG News Service reports that a 32-year-old California man has pleaded guilty on November 20 to charges that he sold thousands of counterfeit chips to the U.S. Navy. (See item **11**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *November 24, WRDW 12 Augusta* – (South Carolina) **Suspects wanted in electrical substation break-in.** Two suspects are wanted by the Aiken County Sheriff's Office

for breaking into an electric substation in Graniteville, South Carolina, on October 9. Surveillance cameras picked up the two after they cut through a fence in an attempt to remove copper from the site. Due to the manner used to cut the wires, investigators believe the two have knowledge of electrical wiring.
Source: http://www.wrdw.com/crimeteam12/headlines/72703257.html

2. *November 24, Associated Press* – (Alabama) **Federal Mine Safety and Health Administration blames low oxygen for Ala. coal mine death.** The federal Mine Safety and Health Administration is blaming low oxygen for the death of a coal miner at a west Alabama mine. The federal Mine Safety and Health Administration said the 53-year-old man and a partner encountered an area of apparent low oxygen during a weekly inspection about 2 a.m. Tuesday at the Jim Walters No. 7 Mine near Brookwood. The second miner and four rescuers were hospitalized as well. The federal agency's spokeswoman says the cause of low oxygen has not been determined. However, MSHA says the men were conducting a weekly examination of a system used to control air flow and dilute methane and other gases and dust. MSHA, Alabama, and the United Mine Workers are investigating.
Source: http://www.wreg.com/news/sns-ap-al--alacoalmineaccident,0,6214650.story

3. *November 24, KSNW 3 Wichita* – (Kansas) **Oil rig catches fire in Pawnee Co.** It is unclear what sparked a huge oil rig fire on the night of November 24 in Pawnee County, Kansas. The fire burned for several hours at an oil field 16 miles west of Great Bend. The rig was not operating at the time and about half of the rig was damaged. No workers were there at the time of the fire.
Source: http://www.ksn.com/news/local/story/Oil-rig-catches-fire-in-Pawnee-Co/64AxYH3Yh0CLgO9_OglWTA.cspx

[Return to top]

Chemical Industry Sector

4. *November 25, Madison Press* – (Ohio) **Ammonia spill closes Route 38.** A hose and coupling on a sprayer traveling on the road in front of the driveway to the Heritage Cooperative depot at 7265 State Route 38 southeast south of London, Ohio, malfunctioned Tuesday afternoon spilling 100 gallons of anhydrous ammonia. The spill sent up a 30-40 foot cloud of the material, created a 5-6-foot wide spot on the road, and a 30-foot rectangular puddle just inside the Heritage driveway. The puddle ran along side the grassy ditch inside the main gravel driveway. The driver was refilling the tanker when the hose and coupling malfunctioned. Firefighters from Central Townships Joint Fire District and Range Township, Madison County EMD, Madison County Sheriff's Office, Ohio State Highway Patrol, Clark County Environmental Protection Agency, the Ohio EPA were on the scene.
Source: http://www.madisonpress.com/local.asp?ID=1851&Story=1

[Return to top]

Nuclear Reactors, Materials and Waste Sector

5. *November 25, Reuters* – (Wisconsin) **NextEra Wisc. Pt Beach 1 reactor back at full power.** NextEra Energy's 514-megawatt Unit 1 at the Point Beach nuclear power station in Wisconsin returned to full power by early Wednesday from 50 percent early Tuesday, the U.S. Nuclear Regulatory Commission said in a report. The company reduced the unit by November 18 to clean the grass off a screen that helps prevent debris in Lake Michigan from getting into the circulating water system. The plant uses the water for cooling.
Source: http://www.reuters.com/article/marketsNews/idUSN2533921120091125

6. *November 24, Philadelphia Inquirer* – (Pennsylvania) **EXC Pa. governor criticizes nuclear plant over handling of alarms.** Naturally occurring radon and a power glitch caused radiation monitors to sound false alarms Monday night and Tuesday morning at the Three Mile Island nuclear plant and caused a fresh round of criticism for the plant's operators from the Pennsylvania governor. The false alarms were in the same Unit 1 containment building where a small contamination incident occurred on Saturday, Exelon Corp. officials said. Though tests showed no abnormal radiation, the governor said Exelon had again failed to notify state emergency-management officials quickly. He said the company did not tell the Pennsylvania Emergency Management Agency until about 9:30 a.m. Tuesday, nearly 13 hours after the first alarm. The alarms sounded in the containment building and were not audible in communities near the plant, which is on the Susquehanna River south of here. All that Three Mile Island officials had to do was telephone the emergency agency and say, "Hey, this is a false alarm ... and we will get back to you as soon as we know that," said the governor, who called such an effort "nothing more than common courtesy. What Exelon folks, at least the Exelon folks at TMI, are not understanding is that the people of Central Pennsylvania, even though this is 30 years old, understandably are very apprehensive and jumpy about all this," the governor told reporters, "and there is no appropriate reason for us not to be notified about this."
Source: http://www.tradingmarkets.com/.site/news/Stock News/2678919/

7. *November 24, San Luis Obispo New Times* – (California) **PG&E seeks to renew Diablo license.** Utility giant Pacific Gas and Electric announced November 24 that it has applied to renew its operating license for the Diablo Canyon nuclear power plant. The PG&E chief nuclear officer did not reveal the price tag on the renewal process, but he said the renewal would cost millions of dollars, in accordance with California Public Utilities Commission regulations, which he did not detail. The current license is set to expire in 2024 and 2025 for Units One and Two of the plant, respectively. The new license, should it be approved, would extend 20 years from those dates. In the next step in the application process, according to PG&E Site Vice President, the Nuclear Regulatory Commission will review PG&E's application and make a decision on the further need for hearings.
Source: http://www.newtimesslo.com/news/3637/pge-seeks-to-renew-diablo-license/

[Return to top]

Critical Manufacturing Sector

8. *November 25, Associated Press* – (National) **Toyota to replace 3.8 million gas pedals.** Toyota Motor Corp. said on November 25 it will replace accelerator pedals on 3.8 million recalled vehicles in the United States to address problems with the pedals becoming jammed in the floor mat. As a temporary step, Toyota will have dealers shorten the length of the gas pedals beginning in January while the company develops replacement pedals for their vehicles, the Transportation Department and Toyota said. New pedals will be available beginning in April, and some vehicles will have brake override systems installed as a precaution. Toyota, the world's largest automaker, announced the massive recall in late September and told owners to remove the driver's side floor mats to prevent the gas pedal from potentially becoming jammed. Popular vehicles such as the Toyota Camry, the top-selling passenger car in America, and the Toyota Prius, the best-selling gas-electric hybrid, are part of the recall. It includes the 2007-10 model year Camry, 2005-10 Toyota Avalon, 2004-09 Prius, 2005-10 Toyota Tacoma, 2007-10 Toyota Tundra, 2007-10 Lexus ES350 and 2006-10 Lexus IS250/350. The recall involving the accelerators was Toyota's largest in the U.S. It was prompted by a high-speed crash in August involving a 2009 Lexus ES350 that killed a California Highway Patrol officer and three members of his family near San Diego. The Lexus hit speeds exceeding 120 mph, struck a sport utility vehicle, launched off an embankment, rolled several times and burst into flames. To fix the problem, Toyota and the government said dealers will shorten the length of the accelerator pedal on the recalled vehicles and in some cases remove foam from beneath the carpeting near the pedal to increase the space between the pedal and the floor. They said owners of the ES350, Camry and Avalon would be the first to receive notification because the vehicles are believed to have the highest risk for pedal entrapment.
Source: http://www.msnbc.msn.com/id/34145358/ns/business-autos/

9. *November 25, Reliable Plant* – (Georgia) **Ga. fiber cement manufacturer faces $128K in OSHA fines.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has proposed $128,560 in penalties against Nichiha USA Inc.'s Macon, Georgia, plant for 27 safety and health violations. "Following a fatality in 2008, OSHA inspected this plant and identified several deficiencies," said the director of OSHA's Atlanta-East Area Office. "Despite management's agreement at the time, our return inspection in 2009 has found that the company continues to endanger its workers' safety and health. The size of these penalties reflects management's failure to address its problems." After inspecting the plant in May and June, OSHA issued citations against the fiber cement manufacturer for 11 repeat safety and health, 11 serious and five other-than-serious violations. Alleged repeat violations from the 2008 inspection include the employer's failure to cover or install guardrails around slurry pits, lack of guards around an exposed chain, and no specific energy control procedures for equipment that had more than one energy source. Employees did not receive adequate training when using corrosive and hazardous chemicals, and the company did not identify, evaluate or provide adequate training for employees working in confined spaces. Emergency eyewashes were not available to employees who worked around corrosive chemicals. The proposed repeat penalty totals $97,760.

Alleged serious violations with proposed penalties of $29,200 include hazards associated with falls, lockout/tagout of energy source, improper storage of compressed gas cylinders, electrical dangers, hazards related to confined spaces and the lack of a bloodborne pathogens program for workers responding to emergencies. Management allegedly committed recordkeeping violations and failed to ensure that workers inspect their full-face respirator for damage, resulting in five other-than-serious violations with penalties totaling $1,600.
Source:
http://www.reliableplant.com/article.aspx?articleid=21473&pagetitle=Ga.+fiber+cement+manufacturer+faces+$128K+in+OSHA+fines

10. *November 24, CNN* – (National) **Toyota recalls 100,000 Tundra trucks.** Federal regulators announced Tuesday the recall of 110,000 Toyota pickup trucks in 20 U.S. states and the District of Columbia. The National Highway Traffic Safety Administration (NHTSA) said that road salts can cause "excessive corrosion" of the Toyota Tundra's frame, which holds a spare tire mounted underneath the vehicle. NHTSA said dislodged spare tires can cause hazards for other vehicles on the road. The corrosion can also damage the rear brake lines and lead to brake system failures, the NHTSA said. The agency urged Tundra owners to remove the spare tires even before taking the vehicles to a dealers to be remedied. The recall involves Tundras from model years 2000 through 2003 that are registered in states where chemical de-icers, such as road salts, are used to treat roadways during the winter. The states included in the recall are: Connecticut, Delaware, Illinois, Indiana, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, New Hampshire, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, Vermont, Virginia, West Virginia, Wisconsin, and the District of Columbia. NHTSA said Toyota will contact owners of affected vehicles and ask that they bring the vehicles to a local dealer to be inspected and repaired. Toyota will either replace the damaged portion of the vehicle's frame, or apply a rust-resistant compound to the affected area, depending upon how bad the corrosion is. Toyota will also contact Tundra owners outside of the United States, according to NHTSA. It was the second major safety problem for Toyota in as many months. In October, the Japanese automaker issued a safety warning for 3.8 million Lexus and Toyota cars because of potentially deadly floor mats.
Source: http://money.cnn.com/2009/11/24/autos/toyota_recall/index.htm?cnn=yes

[Return to top]

Defense Industrial Base Sector

11. *November 24, IDG News Service* – (National) **Man pleads guilty to selling fake chips to US Navy.** A 32-year-old California man has pleaded guilty to charges that he sold thousands of counterfeit chips to the U.S. Navy. In a plea agreement reached on Friday, a Newport Coast, California man pleaded guilty to conspiracy and counterfeit-goods trafficking for his role in an alleged chip-counterfeiting scam that ran between 2007 and 2009. The man, his wife, and her brother operated several microchip brokerage companies that imported chips from Shenzhen, in China's Guangdong province. They

would buy counterfeit chips from China or else take legitimate chips, sand off the brand markings and melt the plastic casings with acid to make them appear to be of higher quality or a different brand, the U.S. Department of Justice said in a press release. Source: http://www.computerworld.com/s/article/9141438/Man_pleads_guilty_to_selling_fake_chips_to_US_Navy

12. *November 24, Marine Corps Times* – (National) **High-capacity magazine may signal demise of SAW.** Marine acquisition officials are considering a high-capacity magazine that could hold 50 or 100 rounds and fit numerous 5.56mm weapons, raising questions about the Corps' plans to move forward with development of the controversial infantry automatic rifle (IAR). Marine Corps Systems Command, based at Quantico, Virginia, is "seeking potential commercial sources for a high capacity magazine for use in a semi or fully automatic rifle," with responses that were due by November 17, according to a new advertisement to industry. The magazine would need to fit "the M16/M4/HK 416 family of weapons," which includes the new 5.56mm auto-rifle SysCom is considering as a replacement for the M249 Squad Automatic Weapon (SAW) in most fire teams. Marine officials did not respond to requests for comment, but adopting a high-capacity magazine for the IAR would address concerns posed by some grunts worried that replacing the SAW with the IAR would cut firepower in situations where a sustained rate of fire is needed. The SAW typically holds a 200-round drum of 5.56mm ammunition, while the IAR is designed for use with 30-round magazines. Source: http://www.marinecorpstimes.com/news/2009/11/marine_iar_112209w/

[Return to top]

Banking and Finance Sector

13. *November 24, KTVB 7 Boise* – (Idaho) **Text message scam targeting bank customers.** Nampa, Idaho, officers say a text message scam is circulating that claims to be an "emergency notification" concerning their bank account – and tries to get the victim to call a toll-free number. When someone calls, they are solicited for account information or charged an extreme amount of money for making the call itself. Police say that the latest round is targeting customers of Mountain Gem Credit Union. Police warn you to ignore the text, and not to give any information out unless you are sure where it is going. If you have questions, you are advised to call your local bank branch. Source: http://www.ktvb.com/news/Text-message-scam-targeting-bank-customers-72748877.html

14. *November 24, DarkReading* – (International) **CSI annual report: financial fraud, malware on the increase.** Malware and financial fraud were among the chief "growth threats" posed to businesses in 2009, according to a new study from the Computer Security Institute that will be published next week. CSI's 14th annual security survey, which will be distributed in conjunction with a free December 1 Webcast, covers a wide range of issues related to security management, including current threats, data loss statistics, and trends in technology usage. Respondents reported big jumps in the

incidence of financial fraud (19.5 percent, over 12 percent last year); malware infection (64.3 percent, over 50 percent last year); denials of service (29.2 percent, over 21 percent last year), password sniffing (17.3 percent, over 9 percent last year); and Web site defacement (13.5 percent, over 6 percent last year). The survey showed significant dips in wireless exploits (7.6 percent, down from 14 percent in 2008), and instant messaging abuse (7.6 percent, down from 21 percent). "The financial fraud was a major concern because the cost of those incidents is so high," says Sara Peters, senior editor at CSI and author of this year's report. Financial fraud costs enterprises approximately $450,000 per incident, according to the study. While financial fraud costs rose in 2009, average losses due to security incidents of all types are down this year — from $289,000 per respondent to $234,244 per respondent, CSI says. Those numbers are still higher than 2005 and 2006 figures. Twenty-five percent of respondents stated the majority of their financial losses in the past year were due to nonmalicious actions by insiders.
Source:
http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=221901046

[Return to top]

Transportation Sector

15. *November 24, Associated Press* – (California) **2 plead guilty to shooting pellet guns at dozens of cars on Calif. freeway.** Two men have pleaded guilty to shooting high-powered pellet guns at dozens of cars on San Francisco Bay area freeways. They were charged in at least 45 shootings on Interstate 680 in Fremont and nine other shootings on Interstate 880. A California Highway Patrol sergeant says most of the cars just had glass broken, but one passenger sustained non-life-threatening injuries when a pellet became lodged in his stomach. The men entered their pleas November 23 to two counts of assault with a deadly weapon and one count of vandalism. They initially faced more than 80 counts.
Source: http://www.latimes.com/news/nationworld/nation/wire/sns-ap-us-freeway-shootings,0,1605562.story

16. *November 24, Associated Press* – (Michigan) **International Bridge Co. files suit against MDOT.** The company that operates the Ambassador Bridge over the Detroit River is suing the state Transportation Department to open ramps leading to local freeways. The Detroit International Bridge Co. said November 24 a lawsuit has been filed with the Michigan Court of Claims. It says transportation officials are "attempting to damage the Ambassador Bridge's business" while supporting a competing project to build a new bridge connecting Detroit to Windsor, Ontario. The suit also says the completed ramps to the Ambassador Bridge have been blocked with dirt and construction equipment. Transportation officials say the Bridge Co. has to complete its part of the project before the ramps can be opened.
Source: http://www.wlns.com/Global/story.asp?S=11568438

17. *November 24, WABC 7 New York* – (New Jersey) **Risky runways at Newark Airport.** A Newark air traffic controller knew instinctively that landing planes on intersecting runways at the same time carried enormous risks, but when the FAA failed to agree, he called for an investigation to make his case. "All we're asking for is the FAA to assist us in doing our jobs," he said. "It's our mandate to keep airplanes from colliding." The two separate landing procedures continued at Newark, as did the close calls. A recently released Department of Transportation Inspector General investigation confirms that the landing on intersecting runways at Newark airport can create "unnecessary flight hazards." The Inspector General also faults the FAA for being "slow to respond." In response to the Inspector General report, the FAA stopped the one landing procedure immediately. On the other runway, landings are now staggered, but the Office of Special Counsel, which also investigated the matter, blasted the FAA for not going far enough and for allowing "a potential danger to the flying public to persist." The FAA says besides staggering planes on approach, and it also plans to add an automated system that will help air traffic controllers separate planes operating on intersecting runways. The agency plans to start that up on December 14th.
Source: http://abclocal.go.com/wabc/story?section=news/investigators&id=7137084

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

Nothing to report

[Return to top]

Water Sector

18. *November 24, Water Technology Online* – (Florida) **FL city adds security to wastewater plant.** A Broward County, Florida, city's wastewater treatment plant now has a new security wall costing nearly $300,000, the South Florida Sun-Sentinel reported November 22. The director of the city's utilities and engineering department said in the story that an existing wall did not fit the bill: It would not have withstood hurricane conditions or acts of terrorism. The $287,567 replacement wall now means the plant is in compliance with federal guidelines that were established after 9/11, he said. The new wall adds security to the city's state-of-the-art wastewater treatment plant. "Since we have so many chemicals on the property, we wouldn't want anyone to have access to them," he said. The city, which maintains 4 million gallons of ground storage at the plant compound, also has two elevated storage tanks.
Source: http://watertechonline.com/news.asp?N_ID=72999

19. *November 24, Patterson Irrigator* – (California) **Wastewater treatment facility fails inspection.** Despite lengthy efforts to improve the quality of Patterson, California's water, a recent inspection of the city's wastewater treatment facility shows state standards are still not being met. The Patterson Water Quality Control Facility received more than a scolding by the Central Valley Water Control Board on November 12, when the board issued a written violation notice — the first for the Poplar Avenue facility, which is responsible for cleansing up to 2.75 million gallons of wastewater every day to produce quality water for disposal. According to the water board, the facility has been out of compliance for more than a year with state limits on contaminant levels in waste discharge. "These are some pretty serious violations," a water board spokeswoman said. "If these levels continue to go untreated, there is a possibility that the contaminants can affect the groundwater over time and even cause health problems for the public. "The levels are nowhere near where they need to be, which is why we're in the process of trying to figure out what they intend to do to fix it." In one problematic treatment tank, nitrogen levels in the water — supposed to be no more than 8 milligrams per liter — were found to fluctuate from a high of 293 in May to a low of 32.2 in August. The same tank's biochemical oxygen demand levels — a measure of the amount of oxygen needed to break down biodegradable substances in the sewage — also fluctuated wildly. In April, levels that were not supposed to exceed 40 milligrams per liter peaked at 172.2. The facility will have until December 15 to respond to the water board with a technical report on how the violations will be fixed. If the problems continue, she said the facility could face several more violation notices before they are fined — a process that could take up to another year.
Source: http://www.pattersonirrigator.com/pages/full_story/push?article-Wastewater+treatment+facility+fails+inspection &id=4751309-Wastewater+treatment+facility+fails+inspection&instance=home_news_lead_story

[Return to top]

Public Health and Healthcare Sector

20. *November 25, WESH 2 Orlando* – (Florida) **Firefighters battle hospital blaze.** Firefighters scrambled to extinguish a blaze at Florida Hospital-Orlando on Wednesday morning. The fire was reported just after 3 a.m. inside the hospital's Medical Plaza. Authorities said they saw heavy smoke coming from a loading dock on the building's ground level. Fire was found inside a laundry room. "Luckily, the doors in the corridor were closed and contained the smoke mostly to the first and second floor. They do have some patients up on the sixth floor that are in-hospital patients. There's smoke up there, and they're not in harm's way. We've already checked on that," an Orlando Fire Department spokesman said. The sprinkler system was activated. Firefighters and doing some cleanup work and trying to determine the cause of the blaze.
Source: http://www.wesh.com/news/21719608/detail.html

21. *November 25, Cherry Hill Courier-Post* – (Connecticut) **Vaccine mandate suspended due to shortage.** Connecticut has suspended a requirement that young children must

receive the seasonal flu vaccine if they attend a child-care facility or preschool facility. The rule — for children ages six months to 59 months — is being suspended due to limited supplies of the needed vaccine, said the state Department of Health and Senior Services. Health officials still are urging that children receive at least one dose of seasonal flu vaccine, if possible.
Source:
http://www.courierpostonline.com/article/20091125/NEWS01/911250354/1006/Vaccine-mandate-suspended-due-to-shortage-

[Return to top]

Government Facilities Sector

22. *November 25, Aerospace Daily and Defense Report* – (Texas) **U.S.A.F. growing cyber warfare ops center.** The newly-created 24th U.S. Air Force, the service's latest numbered force, aims to establish the first elements of a cyberspace command operations center in San Antonio by the end of December. The 24th was stood up in August to conduct cyberspace operations and defend Air Force and other U.S. assets from cyber attack. However, the force does not intend to announce its initial operational capability target until early next year when it clearly understands the task at hand. "Job No. 1 is to create an awareness of the battlespace," says the 24th Air Force commander. Near-term goals include the development of basic defense tactics. "We need to know how to set up and defend the enterprise. It's going to be a crawl/walk/run process," the commander, a major general, says. But there is an underlying urgency to the ramp up. "We're under attack literally every day," he adds.
Source:
http://www.aviationweek.com/aw/generic/story.jsp?id=news/CYBER112509.xml&headline=U.S.A.F. Growing Cyber Warfare Ops Center&channel=defense

23. *November 25, WTKR 3 Norfolk* – (Virginia) **Commissary at Langley Air Force Base briefly evacuated over suspicious package.** On November 24, the 1st Security Forces Squadron responded to a call about a suspicious package at the base exchange. After evacuating the BX and adjacent commissary, the 1st SFS called in threat specialists. The 1st Civil Engineer Squadron Explosive Ordnance Disposal team employed remote means to examine the package. "After confirming the package was not hazardous, we swept the surrounding area to ensure it was clear," said a Staff Sergeant. Deemed as safe, the on-scene commander terminated the incident and lifted the evacuation order at approximately noon.
Source: http://www.wtkr.com/news/wtkr-langley-evac,0,533274.story

24. *November 23, KOTV 6 Tulsa* – (Oklahoma) **Oklahoma state capitol temporarily evacuated due to suspicious package.** The offices of Oklahoma's governor and lieutenant governor were temporarily evacuated November 23 after a man was seen carrying a suspicious package around 2:00 p.m. Other workers at the capitol were also evacuated as a precautionary measure. According to the Oklahoma Highway Patrol, which provides security at the building, the person was interviewed and the brief case

was x-rayed. It was determined the contents of the brief case did not pose a threat. However, the suspect, a 50-year-old male, was arrested by troopers for attempting to by-pass the capitol security checkpoint. All normal activities at the state capitol have resumed.
Source: http://www.newson6.com/Global/story.asp?S=11560264

25. *November 23, U.S. Department of Justice* – (National) **Arrests made in case involving conspiracy to procure weapons, including anti-aircraft missiles.** Arrests were made November 23 in a case involving a conspiracy to procure weapons, including anti-aircraft missiles. A criminal complaint, unsealed today, charged a suspect with conspiring to acquire anti-aircraft missiles (FIM-92 Stingers) and conspiring to possess machine guns (approximately 10,000 Colt M4 Carbines). In addition, the suspect and three other defendants were charged with conspiring to transport stolen goods. Two defendants were charged with conspiring to commit passport fraud. "Keeping missiles, machine guns, and other sensitive U.S. weapons technology from falling into the wrong hands is one of the Justice Department's top priorities. I applaud the many agents, analysts and prosecutors who worked tirelessly to bring about these charges and arrests," said the assistant attorney general for National Security. The investigation was conducted by several agencies working in coordination; including representatives from New Jersey and Pennsylvania law enforcement.
Source: http://www.justice.gov/opa/pr/2009/November/09-nsd-1270.html

For another story, see item **11**

[Return to top]

Emergency Services Sector

26. *November 25, Lowell Sun* – (Massachusetts) **Mass. police probe security-system tampering in wake of cruiser theft.** City police are investigating who tampered with the security system in a police cruiser after a 20-year-old Lowell man stole the vehicle early Saturday morning and led police on a chase before crashing into several parked cars. Police say that while a Lowell Police Officer was responding, along with other officers, to a loud party on Middlesex St. about 2 a.m., he heard a screeching sound. When he looked to see what it was, he spotted someone speeding off in his cruiser. Police say a 20 year old Lowell man, took the cruiser from the street, where it had been left running as the officer responded to the noise complaint. All front-line city police cruisers have a "fail-safe" system that prevents anyone but the officer from driving off with the cruiser, though. The cruiser was inspected the following morning, and that based on a preliminary investigation, it appears someone had tampered with the cruiser's security system, rendering it inoperable.
Source: http://www.policeone.com/police-products/vehicle-equipment/articles/1969455-Mass-police-probe-security-system-tampering-in-wake-of-cruiser-theft/

[Return to top]

Information Technology Sector

27. *November 24, Department of Justice* – (Florida) **Former United Way employee sentenced for damaging charity's computer network.** The acting United States attorney for the Southern District of Florida, and the Special Agent in Charge, Federal Bureau of Investigation, Miami Field Office, announced the sentencing of a defendant on charges of computer fraud. On November 24, a U.S. district court judge sentenced the defendant to 18 months' imprisonment, to be followed by three years of supervised release. In addition, the Court ordered him to pay more than $50,000 in restitution. According to documents filed with the Court, the defendant was a former employee of United Way of Miami-Dade ("UWMD"). He was employed as a computer specialist from July to December 2007. Approximately one year after he left UWMD's employ, the defendant accessed United Way's network without authorization. He deleted numerous files from UWMD's servers and disabled UWMD's telephone voice mail system, which prevented callers from leaving messages for UWMD and prevented UWMD employees from accessing their voice mail accounts. The defendant pled guilty to computer fraud on September 16, 2009.
Source: http://miami.fbi.gov/dojpressrel/pressrel09/mm112409.htm

28. *November 24, GAO Info* – (National) **FBI puts cyber threats in perspective.** The FBI considers the cyber threat against our nation to be one of the greatest concerns of the 21st century. Despite the enormous advantages of the Internet, U.S. networked systems have a gaping and widening hole in the security posture of both our private sector and government systems. An increasing array of sophisticated state and non-state actors have the capability to steal, alter or destroy our sensitive data and, in the worst of cases, to manipulate from afar the process control systems that are meant to ensure the proper functioning of portions of our critical infrastructure. Moreover, the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes continues to rise. When assessing the extent of the cyber threat, the FBI considers both the sophistication and the intent of U.S. adversaries. The most sophisticated actors have the ability to alter our hardware and software along the global supply chain route, conduct remote intrusions into our networks, establish the physical and technical presence necessary to re-route and monitor our wireless communications, and plant dangerous insiders within our private sector and government organizations. The actors that currently have all of these capabilities - which is a finding that is distinct from whether and when they are using them - include multiple nation states and likely include some organized crime groups. The FBI has not yet seen a high level of end-to-end cyber sophistication within terrorist organizations. Still, the FBI is aware of and investigating individuals who are affiliated with or sympathetic to al-Qaeda who have recognized and discussed the vulnerabilities of the U.S. infrastructure to cyber attack, who have demonstrated an interest in elevating their computer hacking skills, and who are seeking more sophisticated capabilities from outside of their close-knit circles. Should terrorists obtain such capabilities, they will be matched with destructive and deadly intent.
Source: http://www.govinfosecurity.com/articles.php?art_id=1962

For another story, see item **29**

Internet Alert Dashboard

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

Communications Sector

29. *November 24, IDG News Services* – (International) **Palm, Sprint pursue lost data from Pre, Pixi.** Palm and Sprint are trying to solve problems some users have had moving data from one Palm webOS device to another, a task that has caused some to lose contacts and calendar entries, according to blogs and online user comments. Users of the Palm Pre and Pixi, the first two devices to run Palm's webOS, can back up contacts, calendar entries, tasks and memos to an online Palm Profile. From that password-protected Web page, they can synchronize that data to another webOS device over the air if they have to change phones for any reason. Normally, one copy of that data resides on the handset and the other in the user's Palm Profile on Palm's servers. But some users who have had to replace or reset their webOS devices have found large amounts of their information missing and apparently irretrievable, according to a post last week on the Palm-oriented blog Pre Central. Several people posted comments on the item, describing data losses. Palm said in a statement it is working with Sprint to solve the problems those users are having. "We are seeing a small number of customers who have experienced issues transferring their Palm Profile information to another Palm webOS device," the company said. "Palm and Sprint are working closely together to support these customers to successfully transfer their information to the new device." It's not the first glitch in online backup for mobile phones. Last month, many users of the T-Mobile Sidekick phone from Microsoft's Danger division lost contacts, photos and other data permanently after a server failure. The incidents could raise concerns among consumers about relying on network-based synchronization instead of backing up data to their own PCs or Macs.
Source:
http://www.computerworld.com/s/article/9141461/Palm_Sprint_pursue_lost_data_from_Pre_Pixi

[Return to top]

Commercial Facilities Sector

30. *November 25, InsideNoVA.com* – (Virginia) **Smoketown Plaza evacuated for gas leak.** A gas leak was reported November 25 at Smoketown Plaza at the intersection of Smoketown and Minnieville roads in Prince William County, Virginia. The stores

inside the center, including a Lowe's hardware store, a grocery and thrift store, were evacuated, sources on the scene said. The gas line that is reported ruptured is an eight-inch distribution line, forcing the evacuation of an "extensive area," said Prince William fire and rescue battalion chief. Police this morning stopped all traffic from entering the Smoketown Shopping Center, and crews from Washington Gas are on the scene working to assess the leak. Firefighters are working to determine if they will need to move their operations command post from the center of the parking lot further away from the storefronts, for safety reasons. They are also checking for other potential leaks in nearby doctor's offices on Golansky Boulevard, near the Woodbridge Post Office. The manager of a grocery store at the plaza said he was not inside the store when it fire crews evacuated it. He said he spoke to his co-workers about the reported gas leak, and he said none of them smelled gas or noticed anything out of the ordinary.
Source:
http://www2.insidenova.com/isn/news/local/article/gas_leak_forces_area_evacuation/47695/

31. *November 24, WEWS 5 Cleveland* – (Ohio) **Ex-doctor injured after bomb explodes in apartment.** A man who formerly worked as an anesthesiologist was injured after an explosion in his Cuyahoga Falls apartment. Now, local and federal investigators are trying to figure out why the man had what is being described as a bomb lab in his home. After the blast, there was another explosive sound. Police said the man injured his hand in the explosions. After the smoke cleared, police said they discovered the source of the explosions: more than four-dozen pipe bombs. Investigators said they also found several firearms. No one knows why the man was living with a small arsenal. The man has yet to be charged with a crime. He was the only person injured in the explosion.
Source: http://www.newsnet5.com/news/21717593/detail.html

[Return to top]

National Monuments and Icons Sector

32. *November 25, Los Angeles Daily News* – (California) **County urges feds to allow night firefighting from air.** The Los Angeles County Board of Supervisors November 23 urged the U.S. Forest Service to allow nighttime air attacks on brush fires. The board cited damage done and momentum gained in the first night of the deadly Station Fire in August, which ended up as the largest wildfire in county history. "County helicopters could have dropped water as needed throughout the night, attempting to control these spots," states a county report. "Such action was not taken because the USFS policy prohibits night flying. Would night flying have made a difference? No one can say for sure, but night flying is a policy change that is needed.'' According to KPCC (89.3 FM), the county is urging a "paradigm shift in wildland fire suppression," including mandating 200-foot brush clearances around strutures, requiring fire-resistant ground covering around the Mount Wilson communication towers, allowing night-flight firefighting, and making sure costs do not get in the way of using the best resources. The county is sending its laundry list to Congress and the U.S. Department

of Agriculture, which oversees the Forest Service.
Source: http://blogs.laweekly.com/ladaily/city-news/county-urges-feds-to-allow-nig/

[Return to top]

Dams Sector

33. *November 24, Springfield Republican* – (Massachusetts) **Dam decision time sought.** The directors of the Belchertown Land Trust are asking Massachusetts for two more years to either repair or demolish the Upper Bondsville Dam, saying the structure is not an imminent threat and they need time to come up with funding for the work. The cash-strapped, nonprofit land trust has been given a deadline of November 30 to submit plans for dealing with the dam, which is rated in poor condition, well below acceptable state standards. Six area legislators have signed a letter sent to the commissioner of conservation and recreation supporting an extension to the deadline and noting that repairing the dam could cost more than $350,000. The president of the trust said that over the past several weeks his organization has had preliminary discussions with some people who own property along the Swift River about the potential for forming some type of association that would be able to contribute money for work on the dam. The 19th century dam was built to power mills that ceased operations decades ago. But it still creates a lake-like impoundment that is appreciated by riverfront property owners in Belchertown, Palmer, and Ware, as well as by many people who use the Swift River for recreational purposes. He said there have also been preliminary discussions with someone who would consider taking ownership of the dam to use for generating electricity. The land trust acquired the dam in 2006 as part of a deal to purchase property on both sides of the river for conservation and recreation purposes. The president said the directors have not voted on whether to repair the dam or take it down but they are aware that community sentiment is strongly in favor of keeping it intact to keep the impoundment.
Source: http://www.masslive.com/metroeast/republican/index.ssf?/base/news-20/1259052617297280.xml&coll=1

34. *November 24, Crossville Chronicle* – (Tennessee) **City OKs dam repairs.** In a short special-called meeting November 19, the Crossville City Council approved a bid for repair of the Caryonah dam but, still could have some potential problems with the Tennessee Department of Environment and Conservation to clear up before moving forward. The council approved the low bid for the dam repair. The low bid totaled $468,509 by Plateau Excavating of Austell Georgia. An engineer also recommended that the city not issue a notice to proceed until proper approval is received from the Tennessee Division of Water Pollution Control. The bid is to remove the top portion of the dam, spread the soil to dry and then rebuild the dam to its specifications. Both the city and their engineering firm are concerned about making sure they have approval for the repair and reconstruction of the dam before they start work on it. The issue of sediment in the creek below the dam was also discussed. It was explained by a city engineer that when the contractor takes over they will be responsible for the pumping of water from the lake that has been costing the city some $10,000 a month. In addition

the contractor will be responsible for erosion control once they are on the job. Source: http://www.crossville-chronicle.com/local/local_story_327165449.html?keyword=topstory

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

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

Department of Homeland Security Disclaimer