Homeland Security

Daily Open Source Infrastructure Report for 9 November 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- The Washington Post reported that on November 5 an army psychiatrist open fired at Fort Hood in Texas, killing 13 people and injuring as many as 31. The suspect was shot by a civilian police officer and remains hospitalized and on a ventilator. (See item **17**)
- According to MSNBC, a suspect was in custody on November 6 after a man opened fire in the offices of an Orlando architecture company that fired him two and a half years ago, killing one person and wounding five others, police and the company said. (See item **26**)

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 6, Reuters* – (Texas) **Shell has temporary upset at Deer Park site.** A temporary process upset in a unit at Shell's Deer Park, Texas, site early Friday morning caused flaring, according to a message on a community information telephone line. A maintenance turnaround at the facility, which began in September, is in the process of ending. The company said that the shutdown and restart of the process units could result in higher-than-normal flaring during the first week of November. It was unclear

from the message if the upset was in the refinery or the chemical side of the facility where Shell operates a 332,000 barrel-per-day joint venture refinery with Mexico's state oil company, Pemex. The facility also has a chemical plant which makes base chemicals used in the manufacture of consumer products. A company spokeswoman was not immediately available for comment.
Source: http://www.reuters.com/article/energySector/idUSN0617537720091106

2. *November 5, Reuters* – (California) **Valero reports Wilmington refinery sulfur unit snag.** Top U.S. refiner Valero Energy Corp on Thursday reported a sulfur unit snag at its 135,000 barrels per day Wilmington, Calif., refinery. "The sulfur monitoring unit tripped off, causing the release," of acid gas, the company said in a filing with the California Emergency Management Agency. Company officials were not immediately reachable for comment.
Source: http://www.reuters.com/article/rbssEnergyNews/idUSN0515242120091106

[Return to top]

Chemical Industry Sector

3. *November 5, WMBD 31 Peoria* – (Illinois) **Chemical accident scare.** A big scare for a local hazmat crew. Two anhydrous ammonia tanks toppled off their trailer and into a ditch at Toute 90 and Duncan Road near Princeville. Peoria's Fire Crews used reverse 911 to call residents to tell them that there could be a leak. But the chemical company was able to transfer the ammonia to another container without a chemical cloud forming.
Source: http://centralillinoisproud.com/content/fulltext/?cid=85512

4. *November 5, Nashville Tennessean* – (Tennessee) **Chemical spill closes Interstate 24 near Briley and 440.** Westbound traffic on Interstate 24 is still partially blocked and the area is expected to be cleared by 7:30 p.m. Interstate 24 westbound, near the Briley Parkway exit, remains shut down due to a chemical spill that happened at 10 a.m. Motorists should avoid I-24 until it re-opens at 2 p.m., according to the Tennessee Department of Transportation. It was a minor spill after a tractor-trailer was forced to slam on its brakes, said an individual of the Nashville Fire Department. No one was injured and the leak was washed down and contained, she said.
Source:
http://www.tennessean.com/article/20091105/NEWS09/91105022/UPDATED++Interstate+24+to+be+partially+blocked+until+5+p.m

[Return to top]

Nuclear Reactors, Materials and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

5. *November 5, WHIO 7 Dayton* – (Ohio) **OSHA wants more fines in West Carrollton explosion/fire.** More fines are now suggested for alleged safety violations at a West Carrollton, Ohio, facility that blew up back in May. The explosion and fire happened at Veolia ES Technical Solutions plant on Infirmary Road.. The Occupational Safety and Health Administration (OSHA) wants additional penalties, adding $64,000 in fines against $45,000 already proposed for a total of $109,000. The company says in a statement, "We have been working diligently since the time of the explosion with all concerned agencies on their investigations, including our own internal inquiry. We will continue to work with OSHA to work through any issues or differences. Our company is dedicated to employee and site safety." Four workers were hospitalized and some $50 million in damage was done.
Source: http://newstalkradiowhio.com/localnews/2009/11/osha-wants-more-fines-in-west.html

[Return to top]

Defense Industrial Base Sector

6. *November 5, Defense News* – (National) **Chilton: 'No doubt' U.S. will eventually field TSAT.** The U.S. Strategic Command chief this week said he is confident the military and industry will one day overcome the technical issues that triggered the Transformational Satellite (TSAT) program's termination and field a next-generation communications platform. The Secretary of Defense in April proposed killing the often-delayed and perennially over-budget program, and Congress has supported the move in 2010 Pentagon spending legislation. But the StratCom chief told reporters Nov. 3 that the concept, as well as the requirements for many of the space-based tools slated for TSAT, are not dead yet. The technological issues that slowed the program and drove its costs to what the Defense Secretary determined were unaffordable levels "are things we can overcome," the StratCom boss said. The military and industry should continue working on things like "routers in space," he said. Once the technology is more mature, "we can then lay in a concrete program where more is known of the technology, the costs." Work has been under way within the Pentagon since April to figure out how to apply the fruit of the multibillion-dollar TSAT development effort to upgrades of existing satellites, such as the military's Advanced Extremely High Frequency constellation.
Source: http://www.defensenews.com/story.php?i=4361752&c=AME&s=AIR

7. *November 5, Nextgov* – (National) **Defense: Open source software is more secure, yes more, than commercial code.** Open source software, freely available program code that the public can download and modify, which many agencies avoid because they view it as a security risk, is often more secure than the alternatives that are commercially developed, a top Defense Department official said on Thursday. The associate director of enterprise services and integration in Defense's Office of the Chief Information Officer helped write a memo issued on Oct. 16 that directed all Defense

agencies to evaluate open source programs on an equal basis with proprietary software and to share open source code internally when appropriate. The department's position on open source, according to the original draft of the memo, is software that goes through a process of peer review tends to be more reliable and secure than software that has not had a similar level of review, according to the offcier. In the end, the final memo emphasized the "positive aspects of open source software that should be considered" by Defense agencies, including a continuous and broad peer-review process enabled by publicly available source code, which "supports software reliability and security efforts through the identification and elimination of defects that might otherwise go unrecognized by a more limited core development team." "If someone hired me to write a piece of code in a proprietary fashion, then a hacker would only have to be smarter than my team to find a weakness," said the founder and executive director of the Open Source Software Institute. "Theoretically in an open source model, where anyone and everyone can review the code, then a malicious hacker must be smarter than all of us. But for federal contractors trying to convince management that open source is a viable option, the challenge is to overcome the perception of liability. The officer calls such a scenario a red herring. "I can have [defense contractors] use this open source code that's proven, or I can pay them to redevelop it, which will introduce a whole bunch of vulnerabilities no one's discovered before," he said. "You're liable whether you write or download [code], or buy proprietary software. If you're a contractor, you're on the hook."
Source: http://www.nextgov.com/nextgov/ng_20091105_5058.php?oref=topstory

[Return to top]

Banking and Finance Sector

8. *November 4, CNET News* – (National) **Congress may require ISPs to block fraud sites.** For the last decade or so, Internet service providers have been dealing with requests to block access to pornographic or copyright-infringing Web sites, or in China, ones that dare to criticize the government. Now a U.S. House of Representatives bill is taking the unusual step of requiring Internet providers to block access to online financial scams that fraudulently invoke the Securities Investor Protection Corporation (SIPC)—or face fines and federal court injunctions. The House Financial Services Committee approved the legislation on November 4 by a 41 to 28 vote. SPIC is a government-linked entity that aids investors when funds are missing from their accounts, up to a limit of $500,000 for stocks, bonds, and mutual funds. Only investor accounts that investors have opened with members of the SIPC—here's a list—qualify for its protection. It turns out that occasionally, Internet fraudsters, scamsters, and other assorted malcontents have posed as legitimate brokerage firms that are SIPC members, often with a similar name or domain name. The scam may be a too-good-to-be-true offer to buy securities that asks the unwitting customer to pay fees in advance, or schemes involving fraudulent checks that eventually bounce. That seems to be in part what prompted a representative from Pennsylvania and chairman of a key subcommittee, to introduce the Investor Protection Act a few weeks ago. Section 508 of that bill says, "Any Internet service provider that, on or through a system or network

controlled or operated by the Internet service provider, transmits, routes, provides connections for, or stores any material containing any misrepresentation (of the SIPC) shall be liable for any damages caused thereby, including damages suffered by the SIPC, if the Internet service provider...is aware of facts or circumstances from which it is apparent that the material contains a misrepresentation."
Source: http://news.cnet.com/8301-13578_3-10390779-38.html

[Return to top]

Transportation Sector

9. *November 5, Plattsburg Press-Republican* – (New York) **Progress made on new ferry around Champlain Bridge.** The states of New York and Vermont are applying for permits to put in a temporary ferry crossing at the Champlain Bridge. The bridge was closed October 16 after an underwater inspection discovered significant concrete erosion of the bridge's piers. The director of planning for the Vermont Agency of Transportation said he is encouraged about the work under way to establish a free, 24-hour temporary ferry about 1,000 feet south of the bridge. "Preliminary information shows this location is likely possible, so long as we can get all the required permits. New York is working on their permits, which hopefully will come about the same time as ours. The location is in the general vicinity of the Bridge Restaurant on Route 17," the director said. He said the ground is staked out with flags and other markings. He said the ferry operation may involve a temporary bridge leading to floating barges that vehicles will drive on to get out far enough into the lake to board the ferry.
Source: http://www.pressrepublican.com/homepage/local_story_309230612.html

[Return to top]

Postal and Shipping Sector

10. *November 4, KOLO 8 Reno* – (District of Columbia) **Scare at Reid office linked to former surgeon general.** A scare at the office of the senate majority leader has been linked to a former surgeon general. The office in Washington, DC was cordoned off when a suspicious letter was delivered to the office Wednesday. It turns out that letter was written by an individual who served under a former U.S. President. The letter included comments about health care reform. It raised suspicions when it was delivered by hand, instead of through the mail. The senator from Nevada was not in his office when the envelope was delivered.
Source: http://www.kolotv.com/home/headlines/69257547.html

[Return to top]

Agriculture and Food Sector

11. *November 6, Associated Press* – (Missouri) **Overnight explosion at AG Processing plant rocks St. Joseph.** A massive blast at a production plant in St. Joseph rocked part

of the city but initial reports were that everyone at the plant escaped injury. KQTV reports that the explosion at the AG Processing Inc. plant occurred around 3:20 a.m. Friday on the city's south side and was felt by residents miles away. First responders say about 25 to 30 employees were working during the explosion, but the blast occurred outside the plant. Emergency crews evacuated nearby businesses. Firefighters contained a small fire to the hydrogen portion of the plant and the fire appeared to be under control by 6 a.m. AG Processing is a farmer-owned cooperative that processes grain into several products from food to renewable fuels.
Source: http://www.kansascity.com/news/breaking_news/story/1552673.html

12. *November 5, U.S Food and Drug Administration* – (National) **FDA and FSIS Collaborate to improve tracing of unsafe food products.** A joint public meeting focused on improving the system for tracing of food products and ingredients that are causing illness outbreaks or presenting other risks to the health of consumers was announced today by the Food and Drug Administration (FDA) of the U.S. Department of Health and Human Services and the Food Safety and Inspection Service (FSIS) of the U.S. Department of Agriculture (USDA). Recognizing the need to increase the speed and accuracy of traceback investigations and traceforward operations, both agencies are building on existing efforts by seeking public input that would help identify elements of effective food product tracing systems, identify current gaps in food product tracing, and suggest specific mechanisms for improvements. The meeting is also intended to improve the ability of FDA and FSIS to use the information in such systems to respond to outbreaks more quickly by rapidly identifying the source of contamination during outbreaks of foodborne illness, and improving the ability of all persons in the supply chain to more quickly identify food that is (or potentially is) contaminated and remove it from the market during traceforward operations. "This public meeting provides an opportunity for FDA to collaborate more closely with FSIS as well as with members of the food industry, many of whom have been making important innovations in food safety practices and technology, and all of whom bear primary responsibility for producing and marketing safe food," said senior advisor to FDA's Commissioner. Food can become contaminated at many different steps in the supply chain. Experience in conducting foodborne disease outbreak investigations suggests that improved product tracing abilities could help identify products associated with disease more quickly, get risky products off the market faster, and reduce the number of sicknesses associated with foodborne illness outbreaks. The meeting will be held Dec. 9 and 10 in Washington at the U.S. Department of Agriculture's South Building in the Jefferson Auditorium, 1400 Independence Avenue, SW, Washington, D.C., 20250.
Source:
http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm189311.htm

[Return to top]

Water Sector

13. *November 5, Fort Myers New-Press* – (Florida) **4 workers injured in Bonita Springs Utility explosion.** Three Bonita Springs Utilites employees and a vendor were injured at a wastewater treatment plant off Morton Ave in Bonita Springs, Florida, on the afternoon of November 5 when a fire sparked for a few seconds at a little before 4 p.m. "Occasionally, you will have pockets of methane and you protect against that with proper ventilation," the Bonita Springs Utilities executive director said. "I'm not really sure what caused the spark." He said his agency will ask the Occupational Safety and Health Administration to investigate. "It's actually a new meter that we were looking at," he said. The four men were being treated at a local hospital. They were expected to recover.
Source: http://www.news-press.com/article/20091105/NEWS0102/91105060/1004/ACC

[Return to top]

Public Health and Healthcare Sector

14. *November 5, CNET News* – (National) **Nation prepares for deadly bat virus.** The U.S. and other countries are investing in Hendra virus (a lethal virus that resides in bat urine and horse spit) research because they fear it may be used in biological warfare, an Australian veterinarian involved in the first Hendra outbreak told horse owners and "bat carers" at the Queensland Horse Council Hendra virus conference last week. The first outbreak occurred in 1994 and killed a prominent Queensland horse trainer and 14 of his horses in 1994. This bug, along with and its even deadlier relative the Nipah virus, is so virulent it's considered a U.S. homeland security threat. There is no effective treatment or vaccine for Hendra or Nipah. The latter has killed hundreds in Malaysia, Bangladesh, and India, while the former has downed four out of the seven people infected in Queensland, Australia—a 57 percent mortality rate. So far it appears that Hendra is transmitted from bats to horses and from horses to humans. Nipah transfers from bats to pigs and from pigs to humans, but there have also been cases of bat to human and human to human transmissions, according to experts.
Source: http://news.cnet.com/8301-13639_3-10391977-42.html

15. *November 5, Los Angeles Times* – (California) **California might miss swine flu inoculation goal because of vaccine shortage.** If H1N1 flu vaccine shortages persist, California may not be able to vaccinate those most at risk by the end of December, public health officials said today. Health officials have said that at least 25 city and county health agencies have received less than 45% of the vaccine doses they ordered. The state's goal had been to have all "high-risk" patients vaccinated by December 31 — but the shortage of vaccine is putting that goal in jeopardy. The epidemiologist for the California Department of Public Health said state officials are monitoring the problem and plan to deliver more vaccine within two weeks to the agencies with significant shortfalls. "As we move forward, we are actually able to tell who has received vaccine, who has not, and try to bring people to parity," he said. In Los Angeles County alone, priority groups include 5.5 million people. Public health officials across the country have said they may have trouble supplying priority groups

with the vaccine by December. The problem, they say, is that the vaccine manufacturing process is taking too long. California was supposed to have received 6.25 million doses of the vaccine by now, but has received about half that, and state officials ordered another 500,000 doses by November 4.
Source: http://latimesblogs.latimes.com/lanow/2009/11/california-might-miss-swine-flu-vaccination-goal-because-of-medicine-shortage.html

16. *November 4, Associated Press* – (New Hampshire) **Social security numbers of medical providers may have been stolen.** Anthem Blue Cross and Blue Shield is warning 10,000 New Hampshire physicians, dentists and other providers that their Social Security numbers may have been stolen. The insurance company says the providers' numbers may be in a file that a national-level employee transferred to a personal laptop computer that was later stolen. A Anthem spokesman says the security breach occurred at a national level and did not include any information about New Hampshire members or their medical conditions. The Blue Cross Blue Shield Association says the employee's actions violated the association's security policies and was unauthorized. The association is offering affected providers free credit monitoring for one year.
Source: http://www.nashuatelegraph.com/News/421085-196/social-security-numbers-of-medical-providers-may.html

[Return to top]

Government Facilities Sector

17. *November 6, Washinton Post* – (Texas) **13 dead in Fort Hood rampage, largest mass shooting on an Army post.** The Arlington-born Army psychiatrist suspected of killing 13 people at Fort Hood Thursday before being shot by a civilian police officer remains hospitalized and on a ventilator, officials said November 6 as investigators probed a motive for the rampage and tried to determine whether anyone else was involved. Military officials said they believe the suspect, a 39-year-old major trained to treat soldiers under stress, opened fire with a pair of pistols — one of them semiautomatic — in the processing facility just after lunchtime. All around him, unarmed soldiers who had been waiting to see doctors scattered or dropped to the floor. A Fort Hood police sergeant responded within four minutes of the report of gunfire, a deputy commander said . The officer arrived just as the suspect was fleeing the building. The suspect fired one of his two guns, hitting the officer in both of her thighs and one wrist, said an officer who witnessed the shooting. The deputy commander said an investigation will determine how the shooter brought guns onto the post, where, like at all U.S. military installations, firearms are kept secured unless they are needed for training or security work. Soldiers and civilians are allowed to maintain privately owned weapons in accordance with local gun laws, the deputy commander said. But they must register those weapons on post.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2009/11/06/AR2009110600897.html?hpid=topnews&sid=AR

18. *November 5, Fox News* – (Washington) **Senior citizens break into military base.** The U.S. Navy is reviewing its security policies following an embarrassing breach this week in Washington State. Five anti-war protesters were able to cut through a perimeter fence around Naval Base Kitsap and walk around the base undetected for four and a half hours. The group included three people in the 60's and three in their 80's. The group was protesting the nuclear weapons kept at the base and hoped to get as close to them as possible. Members claim when they cut through a second and then a third fence they were within fifty yards of a bunker where nuclear warheads are stored. The Navy dismisses that but will not divulge how close the group got to weapons. It only released a statement saying that 'at no time was the safety of Navy personnel, property or the public threatened in any way.' The group was swarmed by Marines and arrested shortly after cutting through the third fence. They were charged with trespassing and destruction of military property, both misdemeanors punishable by up to a year in jail. Naval Base Kitsap is home to a fleet of 11 submarines. Eight of those subs are equipped to fire the trident nuclear missiles. Also, the base reportedly is the storage facility for more than 23-hundred nuclear warheads representing about one-quarter of the nation's nuclear arsenal. The protestors have all been released and are awaiting an initial appearance in federal court.
Source: http://liveshots.blogs.foxnews.com/2009/11/05/senior-citizens-break-into-military-base/?test=latestnews

19. *November 5, KOMU 8 Columbia* – (Missouri) **Radioactive material tracked on campus.** An MU researcher accidentally tracked phosphorus from a lab to a few areas across campus. An unidentified lab researcher accidentally spilled phosphorus-32, a radioactive isotope, at a Schlundt Annex laboratory. The researcher then walked outside, unaware that the chemical spilled onto his or her shoes. Without traveling too far, the researcher realized something was wrong. "(The worker) called the Environmental Health and Safety Department," a MU spokesman said. "They responded right away and were there for several hours." Department workers are using Geiger counters to locate radiation patches. Most of the radiation is in a dirt filled area, at a corner outside Schlundt Annex, the biochemistry building. The radioactive dirt will then be stored for up to six months before it can be disposed. Most of the researcher's footprints have been sealed with black paint to stop any possible contamination from spreading. "We know for sure that there are no personal health risks to anyone in the area," the spokesman said. The risk of airborne exposure to phosphorus-32 is minimal, but it is very dangerous if ingested. The MU Environmental Health and Safety Department and biochemistry students and teachers declined interviews. After the cleanup, an investigation will determine if disciplinary action is necessary.
Source: http://www.komu.com/satellite/SatelliteRender/KOMU.com/ba8a4513-c0a8-2f11-0063-9bd94c70b769/c63b8b0c-80ce-0971-0032-48f091269389

[Return to top]

Emergency Services Sector

20. *November 6, Government Executive* – (National) **House lawmakers seek to remove FEMA from Homeland Security.** On November 5 the House Transportation and Infrastructure Committee approved legislation that would remove the Federal Emergency Management Agency from the Homeland Security Department and return it to independent, Cabinet-level status. The 2009 FEMA Independence Act (H.R. 1174) was first introduced in February by Rep. James Oberstar, D-Minn., and has 29 co-sponsors. The idea of returning FEMA to the independent status it held in the 1990s, before the formation of Homeland Security in 2003, gained traction after the government's bungled response to Hurricane Katrina in 2005. "Putting FEMA in DHS hasn't worked," said the committee's ranking member. "The department has bled FEMA dry of resources, personnel and the authority to manage a large disaster. Elevating FEMA as an independent agency will ensure a clear and direct chain of command from the president." It's not clear if the full House will act on the legislation this session, and it faces an uphill battle in the Senate.
Source: http://www.govexec.com/story_page.cfm?articleid=43991&dcn=todaysnews

21. *November 5, Wheeling Intelligencer* – (West Virginia) **Police assault rifle stolen from vehicle.** A Wheeling Police Department assault rifle may be in the hands of a criminal, the police chief said November 4. The M-16 was stolen on or about October 21 from the vehicle of an off-duty Wheeling officer. The chief said he does not know if the weapon was loaded, but it was taken along with other items removed from the vehicle which was parked outside the city limits. The weapon was issued to a city officer who is a member of the department's SWAT unit. He said the officer claims the weapon was under the back seat of the truck, and the vehicle was locked. The theft is being investigated by the Wheeling Detachment of the West Virginia State Police.
Source: http://www.theintelligencer.net/page/content.detail/id/530558.html?nav=515

[Return to top]

Information Technology Sector

22. *November 6, IDG News Services* – (International) **Gumblar malware's home domain is active again.** ScanSafe researchers are seeing renewed activity regarding Gumblar, a multifunctional piece of malware that spreads by attacking PCs visiting hacked Web pages. Gumblar can steal FTP credentials as well as hijack Google searches, replacing results on infected computers with links to other malicious sites. When the Gumblar malware was found in March, it looked for instructions on a server at gumblar.cn. That domain was taken offline at the time, but has been reactivated within the last 24 hours, wrote a senior security researcher with ScanSafe, on a company blog. Web sites that are infected with Gumblar contain an iframe, which is a way to bring content from one Web site into another. Malware writers usually make those iframes invisible. When a victim visits the site, the iframe will launch a series of exploits hosted on a remote computer to try and hack the visiting machine. Gumblar checks to see if the victim's PC is running unpatched versions of Adobe Systems' Reader and Acrobat programs. If so, the machine will be compromised by a so-called drive-by download.
Source:

http://www.computerworld.com/s/article/9140442/Gumblar_malware_s_home_domain_is_active_again

23. *November 6, IDG News Service* – (National) **Senate committee approves data-breach notification bills.** The U.S. Senate Judiciary Committee has approved two bills that would require organizations with data breaches to report them to potential victims. The Judiciary Committee on November 3 voted to approve both the Personal Data Privacy and Security Act and the Data Breach Notification Act by large majorities. The Data Breach Notification Act, sponsored by a Senator who is a California Democrat, would require U.S. agencies and businesses that engage in interstate commerce to report data breaches to victims whose personal information "has been, or is reasonably believed to have been, accessed, or acquired." The bill would also require agencies and businesses to report large data breaches to the U.S. Secret Service The Personal Data Privacy and Security Act would also require that organizations that maintain personal data give notice to potential victims and law-enforcement authorities when they have a data breach. It would increase criminal penalties for electronic-data theft and allow people to have access to, and correct, personal data held by commercial data brokers. The second bill, sponsored by another Senator who is the Judiciary Committee chairman and a Vermont Democrat, would also require the U.S. government to establish rules protecting privacy and security when it uses information from commercial data brokers. Source: http://www.infoworld.com/d/security-central/senate-committee-approves-data-breach-notification-bills-200

24. *November 6, The Register* – (International) **Backdoor in top iPhone games stole user data, suit claims.** A maker of some of the most popular games for the iPhone has been surreptitiously collecting users' cell numbers without their permission, according to a federal lawsuit filed on November 4. The complaint claims best-selling games made by Storm8 contained secret code that bypassed safeguards built into the iPhone to prevent the unauthorized snooping of user information. The Redwood City, California, company, which claims its games have been downloaded more than 20 million times, has no need to collect the numbers. "Nonetheless, Storm8 makes use of the 'backdoor' method to access, collect, and transmit the wireless phone numbers of the iPhones on which its games are installed," states the complaint, which was filed in US District Court in Northern California. "Storm8 does so or has done so in all of its games." Source: http://www.theregister.co.uk/2009/11/06/iphone_games_storm8_lawsuit/

25. *November 5, DarkReading* – (International) **Little-known hole lets attacker hit main website domain via its subdomains.** Turns out an exploit on a Website's subdomain can be used to attack the main domain: A researcher has released a proof-of-concept showing how cookies can be abused to execute such an insidious attack. A senior researcher for Foreground Security published a paper this week that demonstrates how an exploit in a subdomain, such as mail.google.com, could be used to hack the main production domain, google.com, all because of the way browsers handle cookies. "There's no specific vulnerability here, but it's widening the attack surface for any large organization that has more than one [Web] server set up. A [vulnerability] in any one of those servers can affect all the rest," he says. Most Web developers are not

aware that a vulnerability in a subdomain could be used to target the main domain. "We're trying to get the message out that now you have to treat everything [in the domain] as though someone can compromise your crown jewels," says the CSO for Foreground. "You have to realize that every vulnerability, every attack vector in those subdomains, can be used to compromise [other areas of the domain]," he says. It all boils down to the browsers themselves. Within the DNS architecture, the main domain — fortune500company.com, for instance — has control over its subdomains, such as development.fortune500company.com. Development.fortune500company.com has no authority to change anything on the main fortune500company.com site. But browsers do the reverse, the CSO says. Development.fortune500company.com can set cookies for fortune500company.com, the main domain. That leaves the door open for cookie-tampering, he says, when the subdomain has an exploitable vulnerability, such as cross-site scripting (XSS) or cross-site request forgery (CSRF).
Source:
http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=221600496&subSection=Vulnerabilities+and+threats

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

Nothing to report

[Return to top]

Commercial Facilities Sector

26. *November 6, MSNBC* – (Florida) **1 killed, 5 injured in Fla. shootings; suspect held.** A suspect was in custody on November 6 after a man opened fire in the offices of an Orlando architecture company that fired him two and a half years ago, killing one person and wounding five others, police and the company said. The Orlando police chief identified the suspect as a 40 year old. Police said he was arrested peacefully at his mother's home. All of the victims worked for Reynolds, Smith and Hills, an architecture firm. One was dead and five others were in stable condition at Orlando Regional Medical Center with gunshot wounds, police said.The incident comes just a day after an Army psychiatrist opened fire at Fort Hood, Texas, killing 13 soldiers and wounding 30 others in the worst mass shooting on a U.S. military base. "This is a tragedy, no doubt about it, especially on the heels of the tragedy in Fort Hood that is on our minds," the police chief said. "I'm just glad we don't have any more fatalities or

any more injuries than we currently have."
Source: http://www.msnbc.msn.com/id/33726074/ns/us_news-crime_and_courts/?GT1=43001

27. *November 5, San Diego Union-Tribune* – (California) **Suspicious object under van prompts lot closure.** A suspicious device taped to the bottom of a minivan prompted San Diego police to temporarily close part of the parking lot of a shopping center yesterday afternoon, a spokeswoman said. The driver entered a store at the shopping center near Mira Mesa Boulevard and Reagan Road and returned to find a green bottle taped to the bottom of the driver's side door. After consulting with the bomb squad, authorities determined it was a hoax and removed the bottle, said aspokesman with the San Diego Fire-Rescue Department.
Source: http://www.signonsandiego.com/news/2009/nov/05/suspicious-object-under-van-prompts-lot-closure/

[Return to top]

National Monuments and Icons Sector

28. *November 5, Cape Cod Times* – (Massachusetts) **Ruling could mean delay for Cape Wind project.** A decision on whether to list Nantucket Sound on the National Register of Historic Places is now in the hands of the National Park Service. In a letter sent to the U.S. Minerals Management Service today, the Massachusetts Historical Commission executive director stated that she disagreed with the federal agency's finding that the Sound was not eligible for the listing. A ruling by the National Park Service to list the Sound as traditional cultural property would not automatically kill the proposal by Cape Wind Associates, LLC, to build 130 wind turbines there, but could lead to significant delays in the project's construction. The decision delays any decision by the Interior Department on the proposed Nantucket Sound wind farm by at least 45 days and potentially much longer. Because of the difference of opinion on the listing between the federal and state governments, Minerals Management Service must now seek a formal declaration of eligibility from the National Park Service. Minerals Management Service released a largely favorable environmental report in January that found minor or negligible impacts from the proposed wind farm.
Source: http://www.capecodonline.com/apps/pbcs.dll/article?AID=/20091105/NEWS11/911059965

[Return to top]

Dams Sector

29. *November 6, San Diego Union-Tribune* – (California) **Work to raise San Vicente Dam under way.** Workers are excavating the base of the San Vicente Dam and using high-pressure water to scrape off its face in the first phase of a $588 million project to raise the 66-year-old structure. The San Diego County Water Authority project to raise

the 220-foot dam by an additional 117 is the largest dam raise in the United States. It's also the tallest in the world to use a process called roller-compacted concrete, which can be placed in less time at a cheaper cost, but is as strong as conventional concrete. The project kicked off in July, and is expected to take about three years to complete. The first phase involves hydro-blasting the dam face to remove about 2 inches of concrete to create a bonding surface for new concrete to be added, said the project manager with the San Diego County Water Authority. Workers are also excavating at the base of the dam. The new dam will be widened from 150 feet to 225 feet, and its length will grow from 950 feet to 1,400 feet when completed. After that work is completed next summer, roller-compacted concrete will be added to form a stairstep-like structure on the dam face.
Source: http://www.signonsandiego.com/news/2009/nov/06/work-to-raise-san-vicente-dam-under-way/

30. *November 5, U.S. Geological Survey* – (North Dakota; Minnesota) **Red River flow in Fargo at highest level ever recorded for November.** Recent streamflow measurements show that the Red River in Fargo is flowing at the highest level ever for the month of November. The Red in Fargo was flowing at a rate of 8040 cubic feet per second (cfs) on November 4 making it the highest steamflow recorded for the month of November since measurements were started in the year 1901, according to water scientists with the U.S. Geological Survey. "This is the highest level of streamflow that we have recorded for this time of year since the USGS began monitoring the Red River at Fargo more than 108 years ago," said the director of the USGS North Dakota Water Science Center, which operates a system of stream gauges throughout the state of North Dakota. "It is concerning to see this level of streamflow in November." The USGS operates a network of 65 stream gauges in the Red River of the North Basin to monitor the water level and flow of the river. Through satellite and computer technology, stream gauges transmit real-time information, which the National Weather Service (NWS) uses to issue warnings so local emergency managers can get people out of harm's way. The information is also provided to operators of flood control dams and levees so they can take action to reduce flood impacts.
Source: http://www.usgs.gov/newsroom/article.asp?ID=2344

[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

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.