Homeland Security

Daily Open Source Infrastructure Report for 23 November 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- According to Wired, a health insurer lost 1.5 million patient records last May but waited six months to disclose the incident. The data, which was stored on a portable disk drive that disappeared from the insurer's office, was unencrypted and included patient Social Security numbers, bank account numbers and health data. (See item **16**)
- According to IDG News Services, a Seattle computer security consultant says he has developed a new way to exploit a recently disclosed bug in the SSL protocol, used to secure communications on the Internet. The attack, while difficult to execute, could give attackers a very powerful phishing attack. (See item **25**)

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 19, WPIX 11 New York* – (New Jersey) **1 Injured After NJ Gas Station Explosion.** A northern New Jersey gas station was left in ruins after an explosion the morning of November 19. According to officials, the fire broke out some time before 10:30 a.m. near the intersection of Millburn Avenue and Vauxhall Road. A mechanic

was working on a car when a fire broke out, prompting the explosion, reports said. The worker, who suffered burns to his hands, was transported to St. Barnabus Hospital where he was treated. No other injuries were reported. Investigators have ruled the explosion accidental.
Source: http://www.wpix.com/news/local/wpix-nj-gas-station-explosion,0,4208560.story

2. *November 19, WLKY 32 Louisville* – (Kentucky) **Recommendations made for utility disaster improvements.** The Kentucky Public Service Commission's (KPSC) report on the largest power outages found many ways to improve storm readiness and response. The report, issued on November 19, is based on the KPSC review of the September 2008 wind storm and January 2009 ice storm that caused the two largest power outages in Kentucky's history. Major topics included burial of electric lines, strengthening overhead lines, emergency preparedness and communicating with customers. "There's no magic bullet in here for protecting us from these kinds of events," said the director of communications for the PSC. One issue tackled was the idea of the above-ground utilities clobbered by trees, wind and brought down by ice. "The price tag would be at least $217 billion to bury the electric infrastructure that's above ground in Kentucky today," he said. The PSC said where companies got their lines crossed was communication. The report recommended text alerts, Tweeting, and more real-time updates on restoration. The report estimated windstorm damage costs at $595 million and ice storm costs at $616 million statewide. The commission wants utility companies to look at "hardening the system: stronger wires, poles closer together and other measures to make the grid less susceptible to damage." It has also instituted an underground utility pilot program with a few hundred homes to see how effective the move might be. Utility companies have until March 1 to respond to those recommendations.
Source: http://www.wlky.com/news/21664319/detail.html

For more stories, see items **14** and **17**

[Return to top]

Chemical Industry Sector

3. *November 20, Mobile Press-Register* – (Mississippi) **Pascagoula Mississippi Phosphates plant ordered to correct environmental violations.** It will likely cost about $2.5 million to correct environmental violations cited at the Pascagoula Mississippi Phosphates plant this summer, company leaders said Thursday during a third-quarter conference call. In August, the Environmental Protection Agency (EPA) ordered the company to correct spills, improper storage and other violations found during an inspection by EPA and the Mississippi Department of Environmental Quality (MDEQ). Mississippi Phosphates makes sulfuric acid and phosphoric acid to produce diammonium phosphate, or DAP, fertilizer. The EPA said the plant posed a danger to health and the environment. Violations there include inadequate safety equipment, improper storage, and spills and leaks of solid and liquid wastes. The company said

Thursday that it had spent about $600,000 toward groundwater remediation and expected to spend up to $2.5 million to remedy all the violations. That total does not include any potential civil penalties sought by EPA and MDEQ, said the company's chief executive. To date, the company has "either complied with each and every dictate or submitted a plan of compliance and are awaiting EPA response," he said.
Source: http://blog.al.com/live/2009/11/pascagoula_mississippi_phospha.html

[Return to top]

Nuclear Reactors, Materials and Waste Sector

4. *November 20, Reuters* – (Connecticut) **Dominion Conn. Millstone 2 reactor up to 96 pct.** Dominion Resources Inc's (D.N) 882-megawatt Unit 2 at the Millstone nuclear power plant in Connecticut ramped up to 96 percent by early Friday from 42 percent early Thursday after exiting a refueling outage, the U.S. Nuclear Regulatory Commission said in a report. The unit shut by October 7.
Source: http://www.reuters.com/article/marketsNews/idUSN2010103520091120

[Return to top]

Critical Manufacturing Sector

5. *November 19, Consumer Reports* – (National) **Recall: 2007-2008 Jeep Wrangler.** Chrysler is recalling over 161,000 Jeep Wranglers equipped with automatic transmissions manufactured between June 2006 and July 2007. The vehicles were not equipped with a transmission fluid temperature warning system, and a fire could result if the fluid boils over and comes in contact with the engine or exhaust component. Dealers will inspect the 2007-2008 models and enable a "hot oil" warning light on the dashboard and an audible chime indicating when transmission fluid temperature is elevated. Typically, for the transmission fluid to reach a high temperature in an SUV, the vehicle would need to be used for a heavy-duty purpose, such as serious off-roading or pulling a heavy load. Both scenarios are easy to imagine with a Wrangler, as it excels in its off-road ability. Owners should also be aware of the tow capacity for their Wrangler, which is between 2,000 and 3,500 lbs. depending on the trim line. Those owners who do push their Wranglers hard might also consider an aftermarket transmission cooler.
Source: http://blogs.consumerreports.org/cars/2009/11/recall-20072008-jeep-wrangler.html

6. *November 18, Merrimack Journal* – (New Hampshire) **Fire breaks out at printer manufacturer.** Firefighters are investigating the cause of a small fire that broke out early Wednesday morning at a printer manufacturing company. The fire broke out about 2:56 a.m. at Solidscape Inc., on Daniel Webster Highway. The building's sprinkler system snuffed the fire, and no one was hurt, an official said. The company makes printers used with three-dimensional computer modeling.

Source: http://www.cabinet.com/merrimackjournal/merrimacknews/441231-308/fire-breaks-out--at-printer-manufacturer.html

[Return to top]

Defense Industrial Base Sector

7. *November 19, Aviation Week* – (International) **Lawmakers call for Airbus penalty on KC-X.** Sixteen lawmakers — both Democrats and Republicans — are calling on the Defense Department. to develop a mechanism to penalize a Northrop Grumman/EADS proposal to replace KC-135 refuelers for the U.S. Air Force. The legislators take issue with the process laid out in the Air Force's September draft request for proposals for the KC-X competition. Northrop Grumman/EADS is planning to propose an Airbus A330-based design with Boeing likely to offer a 767 or, possibly, a 777. At issue is the Air Force's proposal not to consider the impact of illegal government aid on the cost of the Airbus-based model. The World Trade Organization (WTO) issued a preliminary ruling in September that said Airbus did benefit from unfair subsidies used to develop its commercial product line. A final ruling from the WTO is expected next year, although final rulings rarely deviate from the findings of a preliminary ruling. A Representative from Washington says there are several ways to account for the illegal subsidies in the competition. He advocates for using the countervailing duty process, which would be used by the Commerce Dept. to calculate a per unit penalty for A330s based on the actual size of the illegal subsidy. This amount, up to $5 million per unit according to another Washington Representative, would then be added by the Air Force to the proposed price of the Northrop Grumman/EADS offering. Northrop Grumman issued a statement supporting the Pentagon's position against accounting for WTO rulings in the KC-X source selection process. "To preemptively force a trade dispute into the tanker procurement process before all outstanding complaints have been fully resolved is a violation of international agreements as well as fundamental WTO rules." Northrop officials did not attend the press conference, saying it was a "nonevent." Source: http://www.aviationweek.com/aw/generic/story.jsp?id=news/KCX111909.xml&headline=Lawmakers Call For Airbus Penalty On KC-X&channel=defense

8. *November 19, Defense News* – (National) **Trials successful for LCS ship.** The U.S. Navy's second Littoral Combat Ship (LCS) successfully completed its acceptance trials November 19, paving the way for the ship to be transferred from its shipbuilder and enter naval service. "Independence performed extremely well during trials," the LCS program manager said in a Navy statement released late Thursday. "LCS 2 conducted two outstanding days at sea. We look forward to delivering this critical asset to the fleet." The Independence left its builder's yard at Austal USA in Mobile, Alabama, on November 16, running at speeds up to 45 knots and demonstrating its systems to a team from the Navy's Board of Inspection and Survey (INSURV). According to the statement released by the Naval Sea Systems Command (NAVSEA), Independence "was presented to INSURV with high levels of completion in production and test. The official results of the trials, including the type and number of trial cards, are currently

being reviewed by the Navy." Construction of the Independence began in November 2005. The ship, like the Freedom from LCS competitor Lockheed Martin, was originally programmed to take two years to build at a cost of $223 million. But a series of miscalculations by the Navy and its contractors, design adjustments and other technical issues doubled the construction time, and the cost for the first-of-class ship has gone over the $700 million mark. Delivery of the Independence is expected in mid-December, with a formal commissioning ceremony scheduled for January 16 at Mobile. Lockheed's Freedom, commissioned a year ago, is now conducting warfare tests, and is expected to carry out its first operational missions next year. In addition to the first two ships, Lockheed and General Dynamics each are working on their second ship. The Navy plans to pick one design in mid-2010 on which to base another 51 LCS ships.
Source: http://www.defensenews.com/story.php?i=4385602&c=AME&s=SEA

[Return to top]

Banking and Finance Sector

9. *November 20, Empire State News* – (National) **Former investment company owner pleads guilty to laundering proceeds of mortgage fraud.** A 35 year old of Albany pled guilty in United States District Court in Albany to a one-count information charging him with the felony offense of laundering of monetary instruments in connection with his role in an extensive mortgage fraud scheme that defrauded financial institutions and other mortgage lenders of over $5.3 million in loans. In court November 19, the guilty party admitted his participation in a mortgage fraud scheme that occurred from at least July 2003 through December 2007, in connection with his former businesses PB Enterprises, Inc., and Greater Atlantic Associates, Inc., located on Central Avenue in Albany. He admitted that, together with others, he knowingly and willfully executed a scheme to defraud banks and other mortgage lenders by arranging to secure excessive mortgages for numerous residential properties in the Capital District through the use of fraudulent loan applications and settlement statements, and by diverting mortgage funds for his personal use, and to others.
Source: http://www.empirestatenews.net/News/20091120-6.html

[Return to top]

Transportation Sector

10. *November 20, Associated Press* – (International) **US wants expedited flier checks expanded.** The Department of Homeland Security wants to expand speedy screening of pre-approved, low-risk air travelers arriving in the United States to most international airports in the country. For more than a year, the department has been testing this program at seven airports across the country and found that participating travelers cut their average waiting time to be screened from 10 minutes to three. The voluntary program, called Global Entry, would be open to U.S. citizens and permanent residents at least 14 years old. They would have to pay a $100 fee and undergo a background check. If accepted into the program, they can go through expedited screening when

they fly into the United States. Ultimately, U.S. Customs and Border Protection, a homeland security agency, plans to expand the program to include foreign travelers whose countries have an acceptable pre-screening process. For instance, people from the Netherlands who are part of that country's Privium program have been accepted into the pilot program. The program will begin at seven airports testing the pilot program and expand to most major international airports. The program allows registered participants to use a self-service kiosk to report their arrival, scan their passport or permanent residency card, submit their fingerprints for biometric verification and make a declaration at the touch-screen kiosk. The kiosk then takes a digital photograph of the traveler as part of the transaction record, issues a receipt and directs the traveler to baggage claim and the exit. Global Entry participants may still be selected randomly by customs officers for additional screening at any time in the process.
Source: http://www.azstarnet.com/allheadlines/318314

11. *November 19, WENN 2 Bartlesville* – (International) **Bomb turns out be fish.** Anti-terror police in Germany closed down an entire terminal at Hamburg airport after mistaking a wrapped package of frozen fish for a bomb. SWAT teams evacuated the terminal after police spotted two plastic wrapped packages that were apparently abandoned. But as the packages began to melt, police say the terminal filled with the unmistakable aroma of rotting seafood. "Luckily just the fish went off, not a bomb," says one officer.
Source: http://www.bartlesvillelive.com/content/weirdnews/story/Bomb-turns-out-be-fish/_F_ftgrjo02ojJ1VZ4kBlw.cspx

For more stories, see items **23** and **30**

[Return to top]

Postal and Shipping Sector

12. *November 20, Reno Gazette-Journal* – (Nevada) **White powder causes brief Post Office closure.** Both of Yerington's Post Office buildings were closed for a little more than two hours Wednesday morning after a white powder substance was found in a mail delivery van at the Post Office at 26 No. Main Street. The Yerington/Mason Valley Fire Department was dispatched to the Main Street Post Office at about 8:50 a.m. Wednesday after two postal employees found a white powder inside of the van. The employees said they did not know which package the white powder had come from. The Main Street Post Office was closed and the facility secured, and Main Street between Broadway and Virginia Street was also closed to traffic. Because the delivery van had come from the South Valley Station Post Office, that location was closed also and all employees were evacuated. No employees at either location reported any medical conditions or injuries, the fire department reported. The Yerington/Mason Valley Fire Hazardous Materials Team made a Level B Hazmat entry at the Main Street Post Office and the box containing the white powder was identified as a "Beer Batter Baking Mix." After approximately two-and-a-half hours, both Post Office

stations were cleared to open.
Source: http://www.rgj.com/article/20091120/MVN01/911200364/1305/BIZ01

[Return to top]

Agriculture and Food Sector

See items **13** and **15**

[Return to top]

Water Sector

13. *November 19, Milwaukee Journal Sentinel* – (National) **Asian carp may have breached barrier.** New research shows Asian carp likely have made it past the $9 million electric fish barrier on the Chicago Sanitary and Ship Canal, a source familiar with the situation told the Journal Sentinel late Thursday. The barrier is considered the last chance to stop the super-sized fish that can upend entire ecosystems, and recent environmental DNA tests showed that the carp had advanced to within a mile of the barrier. That research backed the federal government into a desperate situation because the barrier must be turned off within a couple of weeks for regular maintenance. The plan is to spend some $1.5 million to temporarily poison the canal so the maintenance work can be done. But even as those plans are being finalized, it might already be too late. Now the only thing left standing between the fish and Lake Michigan is a heavily used navigational lock. The Army Corps, along with its state and federal partners in the barrier's design and operation, has scheduled a news conference for 10 a.m. Friday. The fish that can grow to 50 pounds or more are a big deal because they are voracious feeders, overwhelming native species, and they pose a huge hazard to recreational boaters because of their habit of jumping out of the water when agitated by the whir of a boat motor.
Source: http://www.jsonline.com/news/wisconsin/70573047.html

14. *November 18, Patriot-News* – (Pennsylvania) **Twelve Marcellus Shale gas drilling wastewater treatment plants proposed in northern Pennsylvania.** The state Department of Environmental Protection (DEP) is reviewing permit applications associated with at least 12 different proposals to build treatment plants for chemical-tainted wastewater from natural gas drilling operations in northern Pennsylvania. Ten of the plants are proposed in DEP's 14-county north-central region, which is centered on Lycoming and Clinton counties. A professor of biology at Lycoming College and director of its Clean Water Institute, said the flurry of permit applications is evidence of the boom in gas drilling in the Marcellus Shale region of northern Pennsylvania. "The north-central region is almost the hotspot," he said. "They are already drilling a lot now, but over the next number of years we are going to see hundreds and hundreds of wells go in." Water is a huge factor in freeing natural gas trapped in the layer of Marcellus Shale that runs beneath much of the state. After a well is drilled, water mixed with various chemicals and sand is forced down the well to fracture the shale and

release the gas. The process is called hydraulic fracturing, or "fracking." The tainted water that returns to the surface is called "flowback." Disposal of the tainted water is a relatively new and evolving industry in northern Pennsylvania. DEP issued 1,592 Marcellus Shale gas well drilling permits in the first 10 months of 2009. More than one-third of them were in the 14-county north-central region.
Source:
http://www.pennlive.com/midstate/index.ssf/2009/11/twelve_marcellus_shale_gas_dri.html

15. *November 17, Water World* – (Iowa) **Iowa feedlot penalized $25K for alleged waste discharges into river.** A Sioux County, Iowa, cattle feedlot operation has agreed to pay a $25,000 civil penalty to settle allegations that it violated the federal Clean Water Act by allowing manure and wastewater to discharge into the West Branch of the Floyd River. The owner of Schuiteman Feedlots, is the named respondent in the proposed consent agreement and final order placed on public notice today in Kansas City, Kansas. In May 2008, the U.S. Environmental Protection Agency (EPA) inspected Schuiteman's operation and documented that it was confining approximately 3,400 cattle in confinement barns and approximately 1,200 cattle in open feedlots. EPA also documented that Schuiteman's operation was discharging manure and wastewater into the West Branch of the Floyd River. The West Branch of the Floyd River has been on Iowa's list of impaired waters because of low biological diversity and past fish kills. Both of these impacts have been linked to runoff of wastes from concentrated animal feeding operations (CAFOs) such as Schuiteman's feedlot. Under state and federal law, any animal feeding operation that confines 1,000 or more cattle must operate as a "no-discharge" facility, unless it has an approved National Pollutant Discharge Elimination System (NPDES) permit.
Source: http://www.waterworld.com/index/display/article-display/0854526751/articles/waterworld/environmental0/water-pollution_prevention/2009/11/iowa-feedlot_penalized.html

[Return to top]

Public Health and Healthcare Sector

16. *November 19, Wired* – (Connecticut) **Health insurer loses 1.5 million patient records.** A health insurer lost 1.5 million patient records last May but waited six months to disclose the incident. The data, which was stored on a portable disk drive that disappeared from the insurer's office, was unencrypted and included patient Social Security numbers, bank account numbers and health data, according to the Hartford Courant. The disk also contained personal information on at least 5,000 physicians. Health Net discovered the loss in May but never informed patients, law enforcement or government entities, despite data breach laws in some states that require data spillers to notify victims and state officials when residents are affected by a breach. The insurer finally sent a letter to Connecticut's attorney general and the state's Department of Insurance this week. Health Net claimed it took six months to determine what data was on the missing disk. It said that data on the disk was compressed and stored in an image

format that required special software to view, which was available only to HealthNet.
Source: http://www.wired.com/threatlevel/2009/11/healthnet

17. *November 19, KTRK 13 Houston* – (Texas) **Gas leak causes problems at LBJ Hospital.** A gas leak caused problems for patients and staff at LBJ General Hospital in Houston November 19. After hours of searching for the source of the leak, hospital representatives say it was finally capped around 10pm. But it did create some problems at the hospital. The smell of gas was present in the air and as a result of the gas leak, the hospital had to divert ambulances to different hospitals and only accepted walk-ins to the emergency room as they searched for the cause of the leak. Hospital representatives say the leak started around 5pm while construction crews were working on an expansion that would double the ER when they believe they struck a line causing the leak. They have been asking patients, if possible, to go elsewhere. The entire first floor was evacuated except for the emergency room.
Source: http://abclocal.go.com/ktrk/story?section=news/local&id=7128976

[Return to top]

Government Facilities Sector

18. *November 20, CNN* – (California) **Students arrested after 32% tuition hike sparks protests.** Authorities arrested dozens of angry students at the University of California, Davis, campus late Thursday after they refused to vacate the school's administration building in protest of a 32-percent tuition hike. The 52 students were taken into custody by the Davis Police Department and deputies from the Yolo County Sheriff's Department, according to a UC Davis spokeswoman. The arrests at the Mrak Administration building came about four hours after the normal 5 p.m. PT (8 p.m. ET) closing time. At one point, as many as 150 students were at the building protesting the tuition increase, the spokeswoman said. CNN affiliate KCRA captured footage of students outside the building shouting, "Who's university? Our university!" In response to the protests, university officials said they will convene a meeting at noon Friday between students, the director of student affairs and the school's top budget officials.
Source: http://www.cnn.com/2009/US/11/20/california.tuition.protests/

19. *November 20, Columbus Republic* – (Indiana) **Suspicious package leads to Purdue visitor center evacuation.** A Purdue University student has been arrested after a suspicious package led officials to evacuate a visitor information center on the West Lafayette campus. The suspect, of Andover, Massachusetts, was being held Friday on suspicion of criminal mischief and possession of stolen property. He is in the Tippecanoe County Jail in lieu of $10,000 bond. Authorities evacuated about 10 people from the Purdue University Visitor Information Center on Thursday morning after workers reported finding a suspicious box. Police found a wheel lock, a parking ticket and $20 inside. Purdue Parking Services had written the ticket and placed the wheel lock on the student's car that day because it displayed a parking permit that did not belong to him.
Source:

http://www.therepublic.com/main.asp?SectionID=1&SubSectionID=111&ArticleID=139620

20. *November 19, IDG News Service* – (International) **Cyberattacks on U.S. military jump sharply in 2009.** Cyberattacks on the U.S. Department of Defense — many of them coming from China — have jumped sharply in 2009, a U.S. congressional committee reported Thursday. Citing data provided by the U.S. Strategic Command, the U.S.-China Economic and Security Review Commission said that there were 43,785 malicious cyber incidents targeting Defense systems in the first half of the year. That is a big jump. In all of 2008, there were 54,640 such incidents. If cyber attacks maintain this pace, they will jump 60% this year. The committee is looking into the security implications of the U.S. trade relationship with China. It released its annual report to Congress on Thursday, concluding that a "large body of both circumstantial and forensic evidence strongly indicates Chinese state involvement in such activities." "The quantity of malicious computer activities against he United states increased in 2008 and is rising sharply in 2009," the report states. "Much of this activity appears to originate in China."
Source:
http://www.computerworld.com/s/article/9141209/Cyberattacks_on_U.S._military_jump_sharply_in_2009

21. *November 19, Knoxville News Sentinel* – (Tennessee) **IG cites Oak Ridge steroid use, urges DOE to 'consider' expanding drug screens.** The Department of Energy should "consider" the possibility of expanding the drug testing program for employees in the Human Reliability Program, the Inspector General's Office said in a report released during the week of November 16-20. The report cited incidents in which Oak Ridge security guards were found to be using anabolic steroids, and said DOE's past reluctance to expand the screening list - saying it was neither cost-effective nor necessary - may have contributed to delays in discovering the steroid use.
Source: http://www.knoxnews.com/news/2009/nov/19/ig-cites-oak-ridge-steroid-use-urges-doe-consider-/

22. *November 19, KPIX 5 San Fransisco* – (California) **Suspicious package probed in SF Financial District.** The San Francisco Police bomb squad was called out to the Irish consulate on November 19 following reports of a suspicious package. A police spokesman said staffers at the consulate, located at 100 Pine Street, called federal authorities upon discovery of the unidentified package. Federal authorities then called San Francisco Police. The police spokesman also said a diplomatic mission in Los Angeles was recently sent a suspicious package, but no further details were provided. Traffic was being allowed past the scene as police officers investigated.
Source: http://cbs5.com/crime/SF.suspicious.package.2.1323246.html

[Return to top]

Emergency Services Sector

23. *November 19, California State Daily Sundial* – (California) **Explosives brought to local fire station result in closure of Reseda Boulevard.** The Los Angeles Police Department (LAPD) Devonshire and Bomb Squad divisions responded the scene of an incident where explosives were found Thursday evening, resulting in street closures on Reseda Boulevard between Lassen and Plummer Streets. There were no injuries reported. "We were told a man drove up to the fire station, had a car full of explosives and wanted to get rid of them," said an LAPD officer.
Source: http://sundial.csun.edu/2009/11/explosives-brought-to-local-fire-station-result-in-closure-of-reseda-boulevard/

24. *November 19, Charleston Gazette* – (West Virginia) **W.Va. police searching for stolen SWAT rifle, ammo.** Ohio County authorities have not located a fully automatic assault rifle stolen from the Wheeling Police Department almost a month ago. Wheeling's police chief said the full-auto M16 rifle was stolen from the pickup truck of a Wheeling Police SWAT member on October 21 at the officer's home. SWAT team members had been permitted to take their weapons and equipment home with them under police department regulations. An unknown amount of ammunition was also stolen. While it is common practice for law enforcement SWAT team officers to take automatic weapons home or keep them in their vehicles so the weapons are accessible in the event of an emergency, the police chief said he has changed the department's policy on storing automatic weapons since the theft. He said the department's M16s will now be stored at the police station under lock and key.
Source: http://www.policeone.com/police-products/firearms/articles/1967541-W-Va-police-searching-for-stolen-SWAT-rifle-ammo/

[Return to top]

Information Technology Sector

25. *November 20, IDG News Services* – (International) **Security pro says new SSL attack can hit many sites.** A Seattle computer security consultant says he has developed a new way to exploit a recently disclosed bug in the SSL protocol, used to secure communications on the Internet. The attack, while difficult to execute, could give attackers a very powerful phishing attack. The CEO of Leviathan Security Group says his "generic" proof-of-concept code could be used to attack a variety of Web sites. While the attack is extremely difficult to pull off — the hacker would first have to first pull off a man-in-the-middle attack, running code that compromises the victim's network — it could have devastating consequences. The attack exploits the SSL (Secure Sockets Layer) Authentication Gap bug, first disclosed on Nov. 5. One of the SSL bug's discoverers at PhoneFactor says he's seen a demonstration of Heidt's attack, and he's convinced it could work. "He did show it to me and it's the real deal," he said. The SSL Authentication flaw gives the attacker a way to change data being sent to the SSL server, but there's still no way to read the information coming back. The CEO sends data that causes the SSL server to return a redirect message that then sends the Web browser to another page. He then uses that redirect message to move the victim to an insecure connection where the Web pages can be rewritten by the COE's computer

before they are sent to the victim.
Source:
http://www.computerworld.com/s/article/9141206/Security_pro_says_new_SSL_attack_can_hit_many_sites

26. *November 20, The Register* – (International) **IE8 bug makes 'safe' sites unsafe.** The latest version of Microsoft's Internet Explorer browser contains a bug that can enable serious security attacks against websites that are otherwise safe. The flaw in IE 8 can be exploited to introduce XSS, or cross-site scripting, errors on webpages that are otherwise safe, according to two Register sources, who discussed the bug on the condition they not be identified. Microsoft was notified of the vulnerability a few months ago, they said. Ironically, the flaw resides in a protection added by Microsoft developers to IE 8 that's designed to prevent XSS attacks against sites. The feature works by rewriting vulnerable pages using a technique known as output encoding so that harmful characters and values are replaced with safer ones. A Google spokesman confirmed there is a "significant flaw" in the IE 8 feature but declined to provide specifics. It's not clear how the protections can cause XSS vulnerabilities in websites that are otherwise safe. A senior application security engineer at Aspect Security who has closely studied the feature but was unaware of the vulnerability speculates it may be possible to cause IE 8 to rewrite pages in such a way that the new values trigger an attack on a clean site.
Source: http://www.theregister.co.uk/2009/11/20/internet_explorer_security_flaw/

27. *November 20, The Register* – (International) **MS discovers flaw in Google plug-in for IE.** Microsoft has helped discover a flaw in the Google Chome Frame plug-in for Internet Explorer users. The plug-in allows suitably coded web pages to be displayed in Internet Explorer using the Google Chrome rendering engine. Redmond [a Microsoft campus] warned that the plug-in made IE less secure as soon as it became available back in September, an argument bolstered by the discovery of a cross-origin bypass flaw in the add-in Successfully exploiting the flaw creates a means for hackers to bypass security controls though not to go all the way and drop malware onto vulnerable systems. Microsoft and a security researcher are jointly credited with discovering the vulnerability in Google's browser add-on. Google acknowledged the flaw and urged users to update to version 4.0.245.1 of Google Chrome Frame. All users should be updated automatically to the latest version of the software, which also tackles a number of performance and stability glitches. Chief among these are problems handling iFrames, as explained in Google's security advisory.
Source: http://www.theregister.co.uk/2009/11/20/google_plug_in_bug/

28. *November 19, Reuters* – (International) **Chinese military web site target of cyberattacks.** A Web site set up by China's Ministry of Defense this summer was hit by more than 230 million hacker attacks in its first month of operation, but none of the attacks were successful, state media reported on November 19. The China Daily report could not be independently confirmed. If true, that would equate to more than 5,000 attacks per minute. The web site editor told the English-language daily the site had been popular with less malign visitors as well, drawing 1.25 billion visits in the three

months since its August 20 launch. Cyber attacks to steal information or disrupt operations are a growing concern for the world's militaries as technology takes on an ever-increasing role.
Source: http://www.msnbc.msn.com/id/34042775/ns/technology_and_science-security/

29. *November 19, SCMagazine* – (National) **House committee passes cyber R and D, standards bill.** Two draft bills intended to improve the security of cyberspace were combined into one piece of legislation that was passed Wednesday by the House Committee on Science and Technology. The Cybersecurity Enhancement Act of 2009, would support cybersecurity research and development and advance the creation of international cybersecurity standards. "[This legislation] is based on the concept that in order to improve the security of our networked systems, which are fundamentally both public and private in nature, the federal government must work in concert with the private sector," the chairman of the House Committee on Science and Technology, said in his opening statement on November 18. The legislation is a combination of two draft bills that were recently approved by House subcommittees. It incorporates the draft bill Cybersecurity Coordination and Awareness Act, approved in early November by the House Subcommittee on Technology and Innovation, to require the National Institute of Standards and Technology (NIST) to facilitate U.S. involvement in the creation of international cybersecurity standards. The legislation also includes the Cybersecurity Research and Development Amendments Act of 2009, approved in late September by the Research and Science Education Subcommittee, to require federal agencies to submit a long-term research-and-development plan detailing objectives of the initiative and the funding needed to carry it out.
Source: http://www.scmagazineus.com/house-committee-passes-cyber-rd-standards-bill/article/158110/

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

30. *November 19, ComputerWorld* – (National) **FAA glitch shines spotlight on troubled telco project.** The outage of a computer system used by airline pilots to file flight plans in the U.S will likely prompt a closer look at a $2.4 billion telecommunications system that has grappled with numerous problems in the past. The U.S. Federal Aviation Administration (FAA) offered few details Thursday about the exact nature of the glitch, which caused major delays and flight cancellations in airports across the country. But in a statement, the agency blamed a "software configuration problem" within the FAA Telecommunications Infrastructure (FTI) in Salt Lake City. That problem brought

down a system used mainly for traffic flow and flight planning services for about four hours this morning. The flight management system — it's called the National Airspace Data Interchange Network (NADIN) — was affected because it relies on FTI services to operate, the FAA said. There was no indication that the disruption was the result of a cyberattack, the FAA said. FAA experts were investigating the outage and meeting with Harris Corp., the company that manages FTI to "discuss system corrections to prevent similar outages," the agency said.
Source:
http://www.computerworld.com/s/article/9141195/FAA_glitch_shines_spotlight_on_troubled_telco_project

31. *November 17, Periscope IT* – (National) **Fibre-optic cable cut causes website outage.** Thousands of internet users in the United States have been affected by an internet outage, according to reports. Problems were experienced with the ATT.Net homepage on November 16, preventing both webmail and homepage access. After initially failing to comment, a spokesperson for major US telecoms firm AT&T confirmed that an outage was triggered at around 02:30 local time when a fibre-optic cable was cut.
Source: http://www.periscopeit.co.uk/website-monitoring-news/article/fibre-optic-cable-cut-causes-website-outage/544

[Return to top]

Commercial Facilities Sector

32. *November 20, WXIA 11 Atlanta* – (Georgia) **Suspicious package at temple turns out to be newspapers.** The Atlanta Police Department bomb squad was called to the the historic Temple on Peachtree Street in Midtown early Friday morning after reports of a suspicious package. It later turned out to be a bundle of newspapers. Adding to the confusion was the fact the newspapers in question are normally delivered in the afternoon. They are usually brought inside the Temple, but the bundle that caused the concern this morning was left in a main driveway. The package was reported around 6:30 a.m. at the synagogue near the Brookwood Amtrak station. Peachtree Street was shut down from the entrance ramp of I-85 to Spring Street for much of the morning. The incident awakened old memories from the Temple's past. The synagogue, the oldest congregation in Atlanta, was bombed in 1958.
Source: http://www.11alive.com/news/local/story.aspx?storyid=137833&catid=8

33. *November 20, State Journal* – (Ohio) **Entire section of Ohio Valley Plaza is evacuated due to bomb threat.** Belmont County, Ohio sheriff says a man walked into the Factory Card Outlet in St. Clairsville, placed a package on the counter, told the clerk it was a bomb and demanded money Thursday evening. The man, still on the loose, is described as 6-feet, 1-inch tall to 6-feet, 2-inches tall, very thin, wearing a black and white bandanna, blue jeans and a black leather jacket. The sheriff said the man has gray hair and a gray goatee. The sheriff said he had summoned the Columbus Bomb Squad with their bomb detecting K-9s. In the meantime, all the stores in that

section were evacuated. That included Hair Inc., H and R Block, Little Caesars, Picket Fence, Movie Gallery, U.S. Nails and Factory Card Outlet.
Source: http://www.statejournal.com/story.cfm?func=viewstory&storyid=70665

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

34. *November 20, Homeland Security Today* – (National) **New technologies to repair levees.** The Department of Homeland Security (DHS) announced this week that four technologies advanced by the Science & Technology Directorate (S&T), the research arm of DHS, have been tested and passed at the US Department of Agriculture's Agriculture Research Service, Hydraulic Engineering Research Unit in Stillwater, Oklahoma, a facility used by the Army Corps of Engineers to test hydrology equipment and study water flow, dams and levees. DHS has been actively soliciting submissions of ideas and prototypes of new technologies from industry, academia, and government to meet the challenge of quickly closing levee breaches, as well as being suitable for scenarios in which a levee breach may be difficult or impossible to reach with conventional construction equipment. The largest of the technologies, proposed by the Army Corps of Engineers Engineering Research and Development Center in Vicksburg, Mississippi, is a large balloon or tube called the Portable Lightweight Ubiquitous Gasket (PLUG) — light enough to be transported by helicopter and flexible enough to adapt to a wide range of environmental situations. When launched or dropped, the engineers hypothesized, the tube would in quick succession fill with water, float on the flood currents to the breach, and adhere to the breach in the earthen berm or levee that had failed. The directorate's other levee sealing innovations include a smaller version of the PLUG,designed to prevent the over-topping flow of a long, shallow breach. Another technology passing the test was The Rapidly Emplaced Protection for Earthen Levees (REPEL), designed to protect against erosion during the intentional overtopping of levees, mitigating erosion from the back slope of a levee which over time could cause a deep breach. Yet another feasible solution is called The Rapidly Emplaced Hydraulic Arch Barrier (REHAB), an arched tube designed to hold back a surge of water during a levee breach repair, to seal breaches obstructed by debris or other structures, and to be used as a rapidly emplaced surge or flood gate.
Source: http://www.hstoday.us/content/view/11157/149/

35. *November 20, Providence Journal* – (Rhode Island) **Emergency workers train at mock terrorist strike.** The scenario for a practice drill Thursday at the headquarters of the Rhode Island Emergency Management Agency (EMA) involved a hypothetical explosion and a rupture of the main dam at the Scituate Reservoir, creating an

estimated 70-foot wall of water, at its peak, moving down the north branch of the Pawtuxet River. Pretend flooding occurred over swaths of five cities and towns, T.F. Green Airport, and parts of Route 95 — leading to people being stranded on the tops of houses and cars and an unknown number of casualties. Pretending that a lone wolf terrorist had blown a gaping hole in the dam, about 100 emergency management personnel gathered to test the state's public and internal lines of communication, a new 800 MHz radio network, and an emergency action plan mandated by a three-year-old amendment to a state dam safety law. Many more people participated without traveling from federal and state agencies and the municipalities most affected: Scituate, West Warwick, Coventry, Warwick, and Cranston. Among their tasks: Cope with a loss of potable water in the drinking-water system that serves 60 percent of Rhode Island. Among their responses: ask the military to send two water-desalinization plants on barges, have the Poland Spring water company immediately ship hundreds of thousands of liters of bottled water, and activate a little-known mutual aid compact among water systems called RI WARN. Officials said the scenario could occur if there was a catastrophic breach of the Gainer Memorial Dam and a massive release of water into the Pawtuxet River floodplain.
Source: http://www.projo.com/news/content/Gainer_Dam_Drill_11-20-09_HGGH30R_v26.353aa24.html

36. *November 19, Associated Press* – (Nebraska) **Repairs for Lake Maloney dam.** The Nebraska Public Power District (NPPD) hopes to begin repairs soon on the 73-year-old dam holding back Lake Maloney, south of North Platte in western Nebraska. After drawing down the water level, NPPD discovered what it is describing as a separation of the foundation for slope protection. NPPD said the problem must be fixed, but it does not appear to be an emergency. Bids are being sought for the repairs, which NPPD estimated will cost between $4 million and $6 million. Officials hope the work will be finished by April. NPPD said Lake Maloney is a regulating reservoir providing water for the North Platte hydroelectric plant and irrigation downstream.
Source: http://www.omaha.com/article/20091119/NEWS01/911199969

37. *November 19, Associated Press* – (Nebraska) **Probing of Neb. dam finds cracked embankment.** The U.S. Bureau of Reclamation says it will continue to release water from a southwest Nebraska reservoir to relieve stress on a damaged dam. The bureau says it found cracks in the Red Willow Dam's embankment. Engineers have been examining the structure since a sinkhole was discovered in October. The bureau says it will continue to draw down Hugh Butler Lake to just under 2,560 feet for safety reasons and to facilitate the ongoing investigation. Red Willow Dam is 126 feet tall and it forms a reservoir of 85,070 acre-feet. It's located about 11 miles north of McCook. An area manager with the bureau says the move will result in a loss of water supplies for the 2010 irrigation season and affect recreation at the reservoir.
Source: http://www.kotatv.com/Global/story.asp?S=11540099&nav=menu411_2

38. *November 19, Associated Press* – (Missouri; Illinois) **Major levee near St. Louis raising concerns.** The Army Corps of Engineers is monitoring a major Mississippi River levee near St. Louis after discovering a problem that could cause the levee to fail.

Corps officials say the Wood River Levee is not in imminent danger, but the problem is urgent and needs to be fixed. A repair plan and cost estimate have not been determined. The levee protects the Illinois communities of Alton, East Alton and Wood River. Corps officials met Wednesday with local leaders. The corps says "sand boils" were discovered near the Melvin Price Locks and Dam. Sand boils occur when river water on the outside of the levee creates enough hydrostatic pressure to push soil, and water, to the surface on the inside. Eventually, the flow can erode the levee foundation and eventually cause failure.
Source: http://www.wandtv.com/Global/story.asp?S=11537120

39. *November 19, Vail Daily* – (Colorado) **A Dillon Dam security solution?** More than a year after Dillon Dam Road's closure due to unspecified terror threats and the ensuing public outcry, restrictions remain intact as local governments work with Denver Water toward a long-term solution. Members of a security task force are reviewing a recent, confidential assessment of the dam's potential as a terror target while a Representative lobbies for federal dollars to create a permanent security solution. The Representative said the existing "Band-Aid" fix of security guards, limited hours, barriers and buoys calls for a permanent solution. "What we have going on isn't, over the long term, going to make a lot of sense," she said, adding that improvements upwards of $20 million could be a "perfect fit" for U.S. Department of Homeland Security money. But a long-term solution has not been defined — at least not publicly — and members of the task force are wary of speculating. The 231-foot-high earthen dam structure holds 83 billion gallons of water just above Silverthorne and Interstate 70 and is a significant link in Denver's water supply. In July 2008, Denver Water irked local residents and governments when it unexpectedly shut down the Dam Road to public access. The road was opened shortly thereafter, but with limited hours and added security measures.
Source: http://www.vaildaily.com/article/20091119/NEWS/911199959/1078&ParentProfile=1062

[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