Department of Homeland Security Daily Open Source Infrastructure Report for 10 January 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- The Associated Press reported that starting January 31, citizens of the U.S. and Canada ages 19 and older will have to present a government-issued photo ID along with proof of citizenship in order to enter or depart the U.S. by land or sea. Children ages 18 and younger need proof of citizenship, such as a birth certificate. (See items **12**)
- According to Agence France-Presse, an incurable, mosquito-borne dengue disease could spread from subtropical areas into the United States, requiring greater efforts to combat it. While dengue-related illness in the United States "is presently minimal," global warming and poor efforts to control mosquito populations responsible for its spread could accelerate the disease's propagation northward, the experts said. (See item **20**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

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

1. *January 9, Associated Press* – (National) **Oil prices rise on US supply concerns.** Oil prices rose Wednesday amid expectations a U.S. government report will show crude oil stockpiles fell last week. Prices were also supported by fears of further violence in Nigeria, the world's eighth-largest oil producer. Analysts surveyed by Dow Jones Newswires predict crude inventories likely fell 800,000 barrels last week, while supplies of distillates, which include heating oil, likely fell 300,000 barrels. The U.S. Energy

Department's Energy Information Administration will release the report later Wednesday.
Source: http://ap.google.com/article/ALeqM5i5TtajgUpSm7KY5jf-lCJGHBB-tAD8U2DE600

2. *January 9, Business First of Buffalo* – (New York) **Weather change cuts power to thousands.** Tens of thousands of customers of both National Grid and NYSEG were without electricity across Western New York Wednesday as high winds brought a changing weather pattern. National Grid estimated more than 20,000 residences and businesses suffered a power loss as a strong cold front crossed the region overnight. Officials at both companies expect power to be fully restored by late Wednesday night or Thursday morning.
Source: http://www.bizjournals.com/buffalo/stories/2008/01/07/daily23.html

3. *January 8, Daily Record* – (New Jersey) **Squirrel sparks Parsippany-area outage.** Some 386 of residents in Parsippany and Hanover townships, New Jersey, lost power for nearly an hour Tuesday afternoon after a squirrel came into contact with a power line at a substation in Hanover Township. The outage is still under investigation, but the area manager for Jersey Central Power and Light, said it was stemmed from a problem in one of the lines at a substation in Hanover Township. Power was restored by switching to another line, he said.
Source:
http://www.dailyrecord.com/apps/pbcs.dll/article?AID=/20080108/UPDATES01/80108031

[Return to top]

Chemical Industry Sector

4. *January 9, Washington Post* – (New York) **N.Y. pushes to deploy more bioweapons sensors.** New York City officials last month quietly activated some of the nation's newest generation of early warning sensors to detect a biological attack. Five years ago, officials here note, the Bush administration was prodding local authorities to move faster to detect the use of biological weapons and pouring billions into biosecurity-related initiatives. New York's leaders now say the administration's enthusiasm and sense of urgency has flagged in its final year in office. The dispute is partly over whether the new sensors -- each with a $100,000 price tag -- are reliable and affordable enough for widespread deployment. New York City officials wish for more detectors and enhanced capabilities under a federal government program known as BioWatch, under which air samplers were installed in 2003 in more than 30 major U.S. cities to detect the airborne release of biological warfare agents such as anthrax, plague, and smallpox. BioWatch was meant to speed up the response of health authorities in the critical hours before disease could spread and symptoms appeared in people. More than $400 million has been spent so far, but officials in New York and elsewhere say the older air samplers installed under the program do not work as well as intended. Some policy experts and members of Congress take an even more skeptical position, questioning the premises of the BioWatch program. Last month, lawmakers set aside $2 million of BioWatch's $77

million operating budget for a "cost-benefit" analysis by the National Academy of Sciences of whether BioWatch's basic strategy is flawed.
Source: http://www.msnbc.msn.com/id/22567946/

5. *January 9, WMTW 8 Portland* – (Maine) **One hospitalized after mill chemical spill.** One person remains hospitalized following a chemical leak at the New Page paper mill in Rumford, Maine. More than 50 workers on Tuesday were evacuated from the mill after officials said a forklift struck a line carrying a chlorine dioxide solution, which is used for pulp bleaching. Two people were taken to an area hospital. One was treated and released, while the other was held overnight for observation. Officials said fewer than 4 pounds of the chemical were released in the incident, which is not enough to require a report to the Maine Department of Environmental Protection.
Source: http://www.wmtw.com/news/15009570/detail.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

6. *January 9, San Diego Union-Tribune* – (California) **Inspectors plan report on Onofre.** Federal inspectors yesterday said they are scrutinizing the San Onofre Nuclear Generating Station in North County, California, after the failure of an emergency diesel generator in late December. The Nuclear Regulatory Commission said the problem seemed to be caused by an improperly installed electrical connector on the generator. Plant operators fixed the problem, but maybe not quickly enough to meet regulations, the commission said. The agency spokesman said backup generators are important because they supply power to a plant's safety systems if off-site electricity is lost. The San Onofre facility did not have a history of such problems and the December incident did not endanger the public, he said. A statement issued by Southern California Edison downplayed the seriousness of the incident but said the company "welcomes and supports" federal assessments.
Source: http://www.signonsandiego.com/news/northcounty/20080109-9999-1m9onofre.html

7. *January 9, Tech* – (Massachusetts) **Reactor cited for minor violations by Nuclear Regulatory Commission.** The Massachusetts Institute of Technology Nuclear Reactor Laboratory was cited by federal officials for violating regulations, because a worker was exposed to nearly a year's worth of radiation in just one day. According to a U.S. Nuclear Regulatory Commission report, MIT discovered on October 17 that a worker had been exposed to four rems of radiation, or 80 percent of the yearly safe amount. A reading of 0.5 rem or less is typical for the type of work which led to the exposure. The NRC investigated MIT's reactor from October to November. It concluded that MIT had violated two safety requirements at "Severity Level IV," which according to the NRC report means that they have very low safety significance. Violations are assigned a severity level ranging from Severity Level I for the most significant to Severity Level IV for those of more than minor concern, according to the NRC.
Source: http://www-tech.mit.edu/V127/N62/nrc.html

[Return to top]

Defense Industrial Base Sector

8. *January 9, Birmingham News* – (National) **Boeing's interceptor contract leaves systems future in question.** The U.S. Missile Defense Agency is pondering the next steps in the evolution of its system for shooting down enemy missiles fired at the United States. Just how that agency decides to proceed could affect the more than 1,500 Boeing Co. workers in Huntsville, Alabama, that helped design and develop the missile defense system that went online about three years ago. Boeing's work on the project in Huntsville includes program management, engineering, and on-going work to integrate the avionics package with the "kill vehicle" that sits atop each interceptor missile. While there was one contract with Boeing's team to build the initial system, it might not be the case for future work, a Missile Defense Agency spokesman said. The military plans to ask for about $8.5 billion in its budget plan for 2009-2013 for the ground-based missile interceptor system, he said. That includes more interceptor missiles, additional work at the California silos, and about $4.5 billion for a planned European ground-based missile interceptor site, he added.
   Source:
   http://www.al.com/business/birminghamnews/index.ssf?/base/business/1199870287773 10.xml&coll=2

[Return to top]

Banking and Finance Sector

9. *January 9, Red and Black* – (Georgia) **University investigates online security breach.** An overseas hacker broke into a University of Georgia server in December, possibly exposing 4,250 Social Security numbers. The server that was compromised contained Social Security numbers, names, and addresses for prospective, current, and former residents of graduate family housing, according to a news release issued Tuesday afternoon. "Somebody had tried to break in ... but there is no evidence that the numbers have been used. The person may have been there and not known what they had," said the vice president for public affairs in a telephone interview Tuesday afternoon. The university has several security patches and firewalls in place to protect its servers from this kind of breach, the official said, but these defenses occasionally fail to prevent hackers from accessing information. This security lapse marks the fourth time hackers have broken into the university's databases in the past three years. The last incident occurred in February 2007 and exposed 3,500 student Social Security numbers.
   Source:
   http://media.www.redandblack.com/media/storage/paper871/news/2008/01/09/News/Univ-Investigates.Online.Security.Breach-3147814.shtml

10. *January 8, Associated Press* – (Wisconsin) **Printing gaffe riles Wisconsin taxpayers.** A second printing mistake in little more than a year caused about 260,000 Social Security numbers to be put on the outside of envelopes and mailed from a state agency, stunning recipients concerned about the risk of identity theft. The state Department of

Health and Family Services said Tuesday that a private vendor based in Plano, Texas, made the mistake while sending informational brochures for state Medicaid services in the past few days. There have been no reports of any fraudulent activity yet as a result of the mailing.
Source: http://news.yahoo.com/s/ap/20080109/ap_on_re_us/taxpayer_privacy

[Return to top]

Transportation Sector

11. *January 8, City News* – (International) **International flight causes health scare at Pearson Airport.** An Air Canada flight arriving in Toronto from Israel Tuesday night was the source of a major health scare at Pearson International Airport. According to reports, 75 of the 200 people aboard the flight from Tel-Aviv were very ill upon arrival and experiencing serious flu-like symptoms. At least three of the 75 ill passengers, all believed to be part of the same tour group, were taken to hospital with unknown symptoms. There is no word on what tour company they were with, or what their final destination was.
Source: http://www.citynews.ca/news/news_18396.aspx

12. *January 7, Associated Press* – (National) **New border-crossing rules start January 31.** Starting January 31, citizens of the U.S. and Canada ages 19 or older will have to present a government-issued photo ID (such as a driver's license) along with proof of citizenship (such as a birth certificate or naturalization certificate) in order to enter or depart the U.S. by land or sea. Children ages 18 and younger need proof of citizenship, such as a birth certificate. The requirements also apply to Americans driving or sailing to and from Mexico, and to those traveling by sea to and from Bermuda and the Caribbean.
Source:
http://news.yahoo.com/s/ap_travel/20080107/ap_tr_ge/travel_brief_border_crossing;_ylt=AlI.3RyjWQ.rI.e_BGVjW12s0NUE

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture and Food Sector

13. *January 9, Dallas Morning News* – (Texas) **Dallas increasing E. coli inspections after beef stolen.** City health officials are increasing inspections of Dallas food establishments after a federal alert prompted by nearly 15,000 pounds of stolen ground beef that might be tainted with E. coli, officials said. No illnesses have been reported since someone stole a trailer transporting the beef, produced on December 19 by Fort

Worth-based Texas American Food Service Corp., which does business as American Fresh Foods. The trailer was recovered about a week later in southeast Dallas, but most of the beef was gone, officials said. Consumers who have bought products bearing the company name and establishment number "EST. 13116" on the package label should contact the company, according to the U.S. Department of Agriculture's Food Safety and Inspection Service alert. Opened packages should be thrown out and unopened packages set aside, the alert said.
Source: http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/DN-badmeat_09met.ART.State.Edition1.3736e38.html

14. *January 9, Worcester Telegram & Gazette* – (Massachusetts) **State doesn't know if listeriosis outbreak is over.** Though state health officials are hopeful the danger related to contaminated milk from the Whittier Farms processing plant in Shrewsbury, Massachusetts, is contained, they do not know if the listeriosis outbreak is over. The incubation period for listeriosis can be up to 70 days. The state Department of Public Health issued a warning to consumers on December 27 not to drink any milk products from Whittier Farms because of the listeria, which has been linked to the deaths of three men and a woman's miscarriage. On March 6, 70 days will have passed since Whittier was ordered to shut down its milk processing.
Source: http://www.telegram.com/article/20080109/NEWS/801090623/1116

15. *January 8, Food and Drug Administration* – (Texas) **New Era Canning Company announces new recall.** New Era Canning Company of New Era, Michigan, is announcing a new recall to include Mexican style chili beans, green beans, and dark red kidney beans that were shipped to food service and retail customers, because a records review identified the possibility that a small number of cans from each lot may not have been adequately cooked. New Era is recalling these products as a precautionary measure, because cans of vegetables that have not been adequately cooked have the potential for the growth of Clostridium botulinum, a bacterium which can cause botulism, a potentially fatal form of food poisoning.
Source: http://www.fda.gov/oc/po/firmrecalls/newera01_08.html

[Return to top]

Water Sector

16. *January 9, Associated Press* – (Montana) **EPA to reimburse residents who say wells affected by dam cleanup.** The Environmental Protection Agency will reimburse a dozen residents who say their drinking water wells have been affected by the Milltown Superfund cleanup project. Work began in October to remove trainloads of accumulated toxic mud from Milltown Dam on the Clark Fork River near Missoula, Montana. Arsenic and copper are among the contaminants in the mud that was tainted by mining operations upstream in the Butte area. The project is expected to be completed in 2011.
Source:
http://www.montanasnewsstation.com/Global/story.asp?S=7597820&nav=menu227_7

17. *January 8, Palm Beach Post* – (Florida) **$25 million approved to deal with worsening**

drought. Water managers today approved $25 million in emergency spending to deal with the region's deepening drought — including $1.4 million for pumps that could drain Lake Okeechobee nearly dry. The chairman of the board of the South Florida Water Management District said the pumps are essential to meeting the district's obligations to sugar, sod, and vegetable growers who rely on the state's largest lake as their reservoir. The pumps would be a last-ditch attempt to keep water flowing from the lake to neighboring farms during the next five months, the heart of what could be a record-shattering dry season, district leaders said. The rest of the money includes the costs of emergency repairs needed to prevent the abnormally low water levels from causing the collapse of floodgates northwest of the lake.
Source:
http://www.palmbeachpost.com/localnews/content/state/epaper/2008/01/08/0108WATER.html

18. *January 8, Associated Press* – (Georgia) **Georgia panel approves water-use plan.** Faced with severe water shortages after one of the driest years in Georgia's history, officials on Tuesday approved what they hope will be the state's first comprehensive water management plan. The Georgia Water Council unanimously adopted the plan, which must be approved by the state's General Assembly before it can take effect. Georgia has never had a plan that guides how water from lakes, rivers, and aquifers should be divided, but a growing population and the current drought have given the proposal new urgency. The plan approved Tuesday advocates measuring Georgia's water resources and charting how they can be used. It also calls for the establishment of 12 water planning districts to manage state water over the next 50 years. The initial cost of implementing the plan is an estimated $30 million.
Source:
http://ap.google.com/article/ALeqM5iYOMIAzXREFVjcYtNagkheasCXwAD8U20NM01

[Return to top]

Public Health and Healthcare Sector

19. *January 9, San Diego Union-Tribune* – (National) **Rand: Medical-alert responses by agencies dangerously slow.** According to a new study from the Rand Corp., the average response time of U.S. public health departments to medical practitioners' alerts could be dangerously slow. Researchers found that only one-third of the 74 participating agencies consistently connected the reporting doctors or nurses with a qualified "action officer," such as a public health nurse or epidemiologist, within 30 minutes. Even fewer could do so within the 15-minute time frame recommended by the federal Centers for Disease Control and Prevention. The report listed an average response time of 63 minutes, and some agencies took nearly 17 hours to call back. It ranked a third of the health departments as poor because one or more of their reply calls came more than four hours after the alert. The CDC spends up to $1 billion annually to support anti-bioterrorism and emergency-response efforts for public health departments, and it is considering whether to tie future funding with performance benchmarks such as the one tested by Rand. The U.S. Department of Health and Human Services paid for the Rand survey,

which will be published in the February issue of the American Journal of Public Health.
Source: http://www.signonsandiego.com/news/health/20080109-9999-1n9respond.html

20. *January 8, Reuters* – (National) **France best, U.S. worst in preventable death ranking.** France, Japan, and Australia rated best and the United States worst in new rankings focusing on preventable deaths due to treatable conditions in 19 leading industrialized nations, researchers said on Tuesday. If the U.S. health care system performed as well as those of those top three countries, there would be 101,000 fewer deaths in the United States per year, according to researchers writing in the journal Health Affairs. Researchers said such deaths are an important way to gauge the performance of a country's health care system. In establishing their rankings, the researchers considered deaths before age 75 from numerous causes, including heart disease, stroke, certain cancers, diabetes, certain bacterial infections, and complications of common surgical procedures. Such deaths accounted for 23 percent of overall deaths in men and 32 percent of deaths in women, the researchers said.
Source: http://www.reuters.com/article/latestCrisis/idUSN07651650

21. *January 8, Agence France-Presse* – (National) **Incurable dengue disease could spread in U.S.** An incurable, mosquito-borne dengue disease could spread from subtropical areas into the United States as a result of global warming, requiring greater efforts to combat it, health authorities said Tuesday. "Dengue fever, a flu-like illness especially dangerous in children and the elderly, is becoming a much more serious problem along the US-Mexico border and in ... Puerto Rico," said a commentary published in the Journal of the American Medical Association. While dengue-related illness in the United States "is presently minimal," global warming and poor efforts to control mosquito populations responsible for its spread could accelerate the disease's propagation northward, the experts said. The World Health Organization believes 2007 could be on a par with 1998, when nearly 1,500 people died in Asia of dengue fever.
Source:
http://news.yahoo.com/s/afp/20080109/ts_alt_afp/ushealthdengue_080109025121;_ylt=Au7c6nzWXJqtFPyDJO2YpA3Ya7gF

Government Facilities Sector

22. *January 9, KDFW 4 Dallas* – (Texas) B**uilding re-opened after ammonia leak.** In Texas, the Fort Worth Sheriff's Department building has been reopened after an ammonia leak caused emergency crews to respond early Wednesday morning. The room where the leak was discovered had restricted access, according to authorities. The ammonia odor was traced to five cylinders, two of which were corroded. They had been part of a crime scene seizure, according to authorities.
Source:
http://www.myfoxdfw.com/myfox/pages/News/Detail?contentId=5434308&version=7&locale=EN-US&layoutCode=TSTY&pageId=3.2.1

[Return to top]

Emergency Services Sector

23. *January 8, Ohio State University* – (National) **Injuries greater for emergency responders.** New research suggests that at any given time, almost 10 percent of the emergency medical technicians and paramedics in the United States miss work because of injuries and illnesses they suffered on the job. A study examining how common these injuries are and tracking new cases of work-related injuries and illnesses in these professionals also suggests that in one year, an estimated 8.1 of every 100 emergency responders will suffer an injury or illness forcing them to miss work. Compared to data compiled by the U.S. Bureau of Labor Statistics, the rate of injuries requiring work absence among these first responders far exceeds the national average of 1.3 per 100 lost-work injury cases reported in 2006. The study also identified work-related and health conditions most likely to lead to injuries, which included responding to a high volume of emergency calls, working in bigger cities, and having a history of back problems. Researchers conducting the study say that knowing how common severe injuries are in this population will help guide interventions designed to reduce the risks of injury. "There is a relatively high incidence of lost-work injuries among emergency medical services professionals, and those injuries are related to the work they do. We may be able to target specific risks and make changes to see if we can affect those injuries," said the report's first author, a Ph.D. candidate in epidemiology at Ohio State University. "The ultimate goal is to find a way to reduce injuries. But first we have to understand how big a problem it is." The study is published in the December issue of the American Journal of Industrial Medicine.
    Source: http://www.emsresponder.com/web/online/Top-EMS-News/Injuries-Greater-for-Emergency-Responders/1$6819

[Return to top]

Information Technology

24. *January 9, Computerworld* – (National) **New rootkit hides in hard drive's boot record.** A rootkit that hides from Windows on the hard drive's boot sector is infecting PCs, security researchers said today. Once installed, the cloaking software is undetectable by most current antivirus programs. The rootkit overwrites the hard drive's master boot record (MBR), the first sector -- sector 0 -- where code is stored to bootstrap the operating system after the computer's BIOS does its start-up checks. Because it hides on the MBR, the rootkit is effectively invisible to the operating system and security software installed on that operating system. "A traditional rootkit installs as a driver, just as when you install any hardware or software," said the director of Symantec Corp.'s security response team. "Those drivers are loaded at or after the boot process. But this new rootkit installs itself before the operating system loads. It starts executing before the main operating system has a chance to execute." Control the MBR, he continued, and you control the operating system, and thus the computer. According to other researchers, including those with the SANS Institute's Internet Storm Center, Prevx Ltd., and a Polish analyst who uses the alias "gmer," the rootkit has infected several thousand PCs since mid-December, and is used to cloak a follow-on bank

account-stealing Trojan horse from detection, as well as to reinstall the identity thief if a security scanner somehow sniffs it out.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9056378&source=rss_topic17

25. *January 8, IDG News Service* – (National) **Microsoft: Flaw could lead to worm attack.** Microsoft has fixed a critical flaw in the Windows operating system that could be used by criminals to create a self-copying computer worm attack. The software vendor released its first set of patches for 2008 on Tuesday, fixing a pair of networking flaws in the Windows kernel. Microsoft also released a second update for a less-serious Windows flaw that would allow attackers to steal passwords or run Windows software with elevated privileges. The critical bug lies in the way Windows processes networking traffic that uses IGMP (Internet Group Management Protocol) and MLD (Multicast Listener Discovery) protocols, which are used to send data to many systems at the same time. Microsoft says that an attacker could send specially crafted packets to a victim's machine, which could then allow the attacker to run unauthorized code on a system. Security experts say that there is no known code that exploits this flaw, but now that the patch has been posted, hackers can reverse-engineer the fix and develop their own attack code. Because IGMP is enabled in Windows XP and Vista by default, this bug could be used to create a self-copying worm attack, Microsoft said Tuesday.
Source: http://www.infoworld.com/article/08/01/08/Microsoft-flaw-could-lead-to-worm-attack_1.html

26. *January 8, IDG News Service* – (National) **Report: IRS information security still poor.** The Internal Revenue Service continues to have "pervasive" information security weaknesses that put taxpayer information at risk, and it has made limited progress in fixing dozens of problems the U.S. Government Accountability Office (GAO) has previously identified, according to a GAO report released Tuesday. The IRS, the tax-collecting arm of the U.S. government, has "persistent information security weaknesses that place [it] at risk of disruption, fraud or inappropriate disclosure of sensitive information," the GAO report said. The agency, which collected about $2.7 trillion in taxes in 2007, has fixed just 29 of 98 information security weaknesses identified in a report released last March, the new report said. **"**Information security weaknesses -- both old and new -- continue to impair the agency's ability to ensure the confidentiality, integrity and availability of financial and taxpayer information," the GAO report said. "These deficiencies represent a material weakness in IRS's internal controls over its financial and tax processing systems." The GAO has issued multiple reports blasting IRS information security in recent years. The latest report described an IRS data center that took more than four months to install critical patches to server software. At one IRS data center, about 60 employees had access to commands that would allow them to make "significant" changes to the operating system, the GAO said. At two data centers, administrator access to a key application contained unencrypted data log-ins, potentially revealing users' names and passwords. Three IRS sites visited by GAO auditors had computers or servers with poor password controls, the GAO said. The IRS also had lax physical security controls in place for protecting IT facilities, the GAO report said. One

data center allowed at least 17 workers access to sensitive areas when their jobs did not require it, the GAO said. The IRS's acting commissioner said the agency made significant progress in fixing information security problems during 2007, and in a letter to the GAO, said "While we agree that we have not yet fully implemented critical elements of our agency-wide information security program, the security and privacy of taxpayer information is of great concern to the IRS."
Source: http://www.infoworld.com/article/08/01/08/IRS-information-security-still-poor_1.html

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

Nothing to report.

[Return to top]

Commercial Facilities Sector

27. *January 8, Pantagraph* – (Illinois) **Faulty valve cause of anhydrous ammonia leak.** Firefighters were able to shut off a leaking valve on a large anhydrous ammonia tank after suppressing the vapors with water late Monday night at the Evergreen FS grain elevator at Shirley, a Bloomington fire report said Tuesday. Anhydrous ammonia, a form of nitrogen fertilizer used on crops, is extremely corrosive and can chemically burn flesh. The leak was discovered after repair work had been done on the tank. A hazardous materials team from Bloomington's fire department assisted firefighters at the scene of the leak.
Source: http://www.pantagraph.com/articles/2008/01/08/news/doc47840e4a497b6873799570.txt

[Return to top]

National Monuments & Icons Sector

28. *January 8, Pensacola News Journal* – (Florida) **Vandals deface memorials.** Two war monuments at Veterans Memorial Park in Pensacola, Florida, have been vandalized with spray paint. Swastikas, foul language, and illegible writing were sprayed with black paint on both the World War I monument and the Purple Heart monument. Damage is estimated to be about $1,000, the Pensacola Police Department said.

Source: http://www.pensacolanewsjournal.com/apps/pbcs.dll/article?AID=/20080108/NEWS01/801080326

[Return to top]

Dams Sector

29. *January 8, Journal and Courier* – (Indiana) **NIPSCO says dams are structurally sound.** On January 8, the Northern Indiana Public Service Company officials said the Norway and Oakdale dams are structurally sound, contradicting an earlier report by the National Weather Service. Earlier in the day, there were reports that the two dams on the Tippecanoe River might have structural damage as flood waters climbed. That morning, more than 26,000 cubic feet of water per second was flowing through the dams. The previous record for both dams was approximately 22,000 cubic feet of water per second. Typically, flooding begins to occur around the 14,000 mark, the director of communications and public affairs for NIPSCO, which owns the dams, said.
Source: http://www.jconline.com/apps/pbcs.dll/article?AID=/20080108/NEWS09/80108024

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Subscription and Distribution Information:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

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

Department of Homeland Security Disclaimer