Department of Homeland Security Daily Open Source Infrastructure Report for 9 January 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- According to WVEC 13 Hampton Roads, two pipe bombs found on railroad tracks in Newport News, Virginia, over the weekend were safely detonated. (See items **15**)
- IDG News Service reported that Symantec Corp. said U.S. government agencies need to take additional steps to protect against cybersecurity problems after a series of congressional hearings and reports exposed several weaknesses in 2007. The U.S. Government Accountability Office also issued about a dozen reports in the last six months criticizing federal agencies for not fully implementing the GAO's cybersecurity recommendations. (See item **31**)

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 8, Reuters* – (International) **Iraq says refinery's output not affected by fire.** A fire at Iraq's largest oil refinery, which killed one employee and injured others, has not affected production at the Baiji refinery in northern Iraq, the Oil Ministry said on Tuesday. The refinery was producing fuel and oil derivatives with a capacity of more than 200,000 barrels per day after Monday's fire, which was sparked by a technical fault. Some units at the refinery had been stopped for precautionary measures but were back online on Tuesday. A chief engineer was killed and many workers injured in the

blaze, which engineers at the refinery told Reuters on Monday was caused by an explosion that destroyed the liquefied petroleum gas unit. The ministry statement did not say whether the LPG unit was destroyed. A ministry spokesman said engineers were evaluating the extent of the damage caused by the fire.
Source: http://www.guardian.co.uk/feedarticle?id=7207436

2. *January 6, Associated Press* – (Montana) **Canadian operator of Montana Refining eyes expansion.** Connacher Oil and Gas of Alberta, Canada, is considering a 15,000-barrel-a-day expansion at Montana Refining Co. in Great Falls. Montana Refining, which is currently equipped to handle a daily 10,000 barrels of oil, is set up to process heavy oil. That is noteworthy because oil sands production in Alberta is taxing North America refineries' capacity to handle heavy crude.
Source: http://www.montanasnewsstation.com/Global/story.asp?S=7585099

[Return to top]

Chemical Industry Sector

3. *January 7, WTVH 5 Syracuse* – (New York) **Chemical spill in Madison County.** Two people were hospitalized Monday morning after a hydrochloric acid spill at the Cornell biological field station in Madison County on the southern shore of Oneida Lake. The facility serves as the primary aquatic research center for Cornell University. The two workers were moving the acid and spilled around two and a half liters of it. Both were having difficulty breathing after the spill, but are expected to be okay.
Source: http://www.wtvh.com/home/related/13502937.html

4. *January 7, WREX 13 Rockford* – (Minnesota) **Tiny town evacuated after train derailment and chemical leak.** A tornado derailed 8 train cars in McHenry County and police subsequently found a leak near a container holding ethylene oxide, a chemical used to sterilize food or medical supplies. Police issued a mandatory evacuation for Lawrence and the surrounding area and urged people to stay away from their homes if the homes were in the area of the spill.
Source: http://www.wrex.com/News/index.php?ID=25330

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *January 7, Associated Press* – (Ohio) **Small pipe leak found at nuclear plant.** Workers found a small radioactive water leak inside a nuclear power plant that was shutdown for maintenance in December, plant operator FirstEnergy Corp. said Monday. The leak was on a weld that held two pieces of cooling pipe inside a reactor containment building at the Davis-Besse nuclear plant along Lake Erie, FirstEnergy said in a report filed with the Nuclear Regulatory Commission. The amount of water was so small that it was almost unnoticeable when discovered Friday, said a FirstEnergy spokesman. "It involved water from the reactor, so it is radioactive water, but it is within the containment building and nothing was released. Our workers were not affected," he said. The spokesman had no

estimate on how long the evaluation of the leak may take or how long the plant will remain shut down.
Source: http://www.businessweek.com/ap/financialnews/D8U1BPLO0.htm

6. *January 7, Reuters* – (New York) **URS wins $67 million U.S. nuclear demolition contract.** Engineering and construction firm URS Corp. said on Monday the U.S. Department of Energy awarded its Washington unit a $67 million contract to deactivate, demolish, and remove process facilities and nearby contaminated soil from the Separations Process Research Unit, a former nuclear research facility in Niskayuna, New York. SPRU was operated from 1950 to 1953 as a pilot plant to research chemical processes to extract uranium and plutonium from irradiated uranium.
Source: http://www.reuters.com/article/tnBasicIndustries-SP/idUSN0743025820080108

7. *January 6, Los Angeles Times* – (National) **Elite teams prepare for nuclear terrorism.** Since the September 11, 2001 attacks the Office of Emergency Response at the National Nuclear Security Administration has created 26 rapid-response units. If a nuclear device is found, two other specialized teams would rush to the scene, one from a base in Albuquerque, New Mexico, where a fueled jetliner is on 24-hour alert, the other from rural Virginia. The teams would first try to disable a bomb's electrical firing system and then quickly transfer the weapon to the Nevada desert. There, the bomb would be lowered into the G Tunnel, a 5,000-foot shaft, where a crew of scientists and FBI agents would try to disassemble the device behind steel blast doors and log the evidence. About 1,000 nuclear weapons scientists and an additional 500 to 1,000 FBI professionals participate in the effort, though not full time. Increased investment in the project reflects an acknowledgment that the nation is vulnerable to terrorists seeking to plant a nuclear device. The report due next month is a major technical and policy analysis of the approach and is being conducted by some of the nation's top nuclear-weapons experts. Officials hope that nuclear forensics will allow scientists to assess the size of a detonation within one hour, the bomb's sophistication within six hours, how its fuel was enriched within 72 hours and the details of national design within a week, said a retired weapons scientist working on the forensics study.
Source:
http://www.statesman.com/news/content/news/stories/nation/01/06/0106nuclearteams.html

8. *January 5, Knoxville News Sentinel* – (Tennessee) **Feds confirm 2006 security violation at Oak Ridge nuclear plant.** Federal inspectors have confirmed a late 2006 security breach, in which an unauthorized laptop computer was taken into a high-security area at the Y-12 nuclear weapons plant. They also found that Y-12's cyber security personnel did not respond properly after the breach was discovered. The report released Friday by the Department of Energy's Office of Inspector General said there may have been dozens of similar security violations in recent years involving the use of unauthorized laptops in "limited areas" at Y-12. The investigation began after the Inspector General's Office received an allegation that a security breach was not properly reported. According to the IG report, Y-12's cyber security staff did not respond properly, "thereby allowing the user to depart the limited area with the laptop

computer." That was contrary to DOE policy and prevented collection of evidence, the report said. Also, the incident was not reported to DOE headquarters in Washington until six days later, the report said. There is a 32-hour reporting requirement. The Inspector General said a number of corrective actions were taken following the October 2006 incident. For instance, the federal manager at Y-12 "required that the involved individuals be removed from the Y-12 site and their unclassified computer accounts suspended." The plant's federal overseers agreed with the recommendations, such as "refresher" training for all employees on security requirements and holding accountable all violators.
Source: http://www.knoxnews.com/news/2008/jan/05/feds-confirm-2006-security/

[Return to top]

Defense Industrial Base Sector

9. *January 8, Business Wire* – (Georgia) **Tri-S Security subsidiary awarded $58.0 million contract for federal facilities in state of Georgia.** Tri-S Security Corp., a provider of security services and equipment for government and private entities, today announced its wholly-owned subsidiary, Paragon Systems, Inc., was awarded on December 31, 2007, a new contract with the U.S. Department of the Homeland Security, for the state of Georgia, for $58.0 million. Paragon will begin the contract April 1, 2008, and the contract will run for five years at an estimated $11.6 million per year. Paragon will provide security for federal government facilities throughout the state of Georgia. Over 250 armed security guards will be deployed throughout the state. This award increases the total awards for Paragon to more than $146.2 million for the year ending December 31, 2007, surpassing its 2006 contract awards of $72.7 million by an increase of 101 percent.
Source: http://www.foxbusiness.com/markets/industries/finance/article/tris-security-subsidiary-awarded-580-million-contract-federal-facilities-state_427522_9.html

10. *January 7, Philadelphia Business Journal* – (National) **Boeing submits new bid for $10 billion helicopter contract.** Boeing Co. said Monday it has submitted its revised bid for the $10 billion Combat Search and Rescue helicopter contract to the Air Force. The St. Louis company won the contract in November 2006, but its competitors lodged protests that were sustained by the Government Accountability Office, and the Air Force reopened the bidding. Boeing is proposing building a helicopter called the HH-47, which it is calling an "advanced derivative" of the Chinook helicopter that it makes at its factory in Ridley, Pennsylvania. Boeing said the HH-47 shares many of the features of the modernized Chinooks, the CH-47 and MH-47G, it is turning out in Ridley now.
Source: http://www.bizjournals.com/philadelphia/stories/2008/01/07/daily10.html

[Return to top]

Banking and Finance Sector

11. *January 8, WLNS 6 Lansing Jackson* **–** (Michigan) **Bank scam warning.** A warning was distributed to members of the Lansing Automakers Federal Credit Union (LAFCU),

who are targeted by scammers using a phony email. A union official said "They are putting a phone number out there, a fictitious phone number for our members to call, or the consumer to call, and it asks for you to put in credit card information." That phone number comes in an email that leads people to believe the credit union is deactivating their bank card. The phony email asks the recipients to respond by calling a phony telephone number. Credit union officials say they do send out emails, but never ask recipients to respond. LAFCU is working with authorities to shut down the fake telephone number.
Source: http://www.wlns.com/Global/story.asp?S=7592139&nav=0RbQ

12. *January 8, WGAL 8 Lancaster* – (Pennsylvania) **Scammers call local phones claiming to be bank.** The Bank of Lancaster County is issuing new account numbers to some of its customers victimized by a weekend telephone scam. Instead of targeting victims in an e-mail scam, the con artist tried a more personal approach by calling them on the phone, and unfortunately some people fell for it. Most people who received the message were asked to dial a number in area code 717 and to give their debit card number, expiration date, and their pin. The phone scam actually started as a case of computer fraud. According to a bank spokesman, their investigation shows that the scam artist apparently hacked into a white pages directory and somehow captured all phone numbers listed for Lancaster County. The scammer then hacked into a second computer system that is an automated dialing service.
Source: http://www.msnbc.msn.com/id/22543446/

13. *January 7, KESQ 3 Palm Springs* – (California) **BBB logo involved in foreclosure scam.** San Bernardino County officials are alerting residents about a scam targeting homeowners facing foreclosure. In it, companies are using the Better Business Bureau logo to convince homeowners they can save them from foreclosure. The county assessor said these companies are preying on vulnerable homeowners, stealing $500 to $1800 each time, according to foreclosure specialists. The scams offering loans and title transfers that claim to stop foreclosure come in envelopes bearing the Better Business Bureau logo with ads claiming to fix foreclosure problems. The Better Business Bureau has tried to stop the unauthorized use of their logo because it is often enough to draw in vulnerable homeowners. Because the civil courts are so overloaded, recovering any damages could take years.
Source: http://www.kesq.com/Global/story.asp?S=7590367&nav=9qrx

[Return to top]

Transportation Sector

14. *January 8, KRTV 3 Great Falls* – (Montana) **Jet diverted to Great Falls following fire scare.** A commercial flight carrying nearly 170 people was forced to make an emergency landing in Great Falls on Monday morning. The United flight was heading from Seattle to Chicago's O'Hare airport when a small fire ignited in one of the bathrooms. The plane landed safely at the Great Falls International Airport at around 8:30 a.m. The airport director said a crew member quickly extinguished the flames while the plane was in the air.

Source:
http://www.montanasnewsstation.com/Global/story.asp?S=7587471&nav=menu227_6/global/story.asp?s=3557224

15. *January 7, WVEC 13 Hampton Roads* – (Virginia) **Pipe bombs found on railroad tracks.** Two pipe bombs found on railroad tracks in Newport News, Virginia, over the weekend were safely detonated. Police responded to the tracks near the James River Bridge Saturday around 2:00 p.m. By nightfall, a second device had been found, so authorities had to stop train traffic until the situation was cleared.
Source:
http://www.wvec.com/news/topstories/stories/wvec_local_010708_nn_pipe_bombs.1a8e5fe2.html

16. *January 7, Reuters* – (West) **Product safety chief targets West Coast ports.** Major shipping ports on the West Coast, such as Seattle and Long Beach, California, will be the first targets of a new import surveillance program detailed on Monday by the Consumer Product Safety Commission (CPSC). The CPSC acting chairman said the program for the first time will permanently assign agency personnel to key ports full-time. The CPSC will combine its surveillance efforts with a new cargo tracking system being implemented along with the U.S. Customs and Border Protection service, which will give CPSC personnel data about "shipments bound for the U.S. even before they leave foreign ports," with a focus on high-risk products, she said.
Source:
http://news.yahoo.com/s/nm/20080107/us_nm/productsafety_nord_dc;_ylt=Asx6LNd1bqCTn2suEDBLKBQWIr0F

[Return to top]

Postal and Shipping Sector

17. *January 7, Monroe Evening News* – (Michigan) **Suspicious package reported at office.** Shortly after noon on January 7 in Monroe, Michigan, a security guard notified authorities when he came across a suspicious package left at the new Social Security office. The area was cordoned off and the public was not allowed to enter the building. Officials have cleared the scene and the area has since been reopened after a police dog determined the package did not contain explosives. The parcel was delivered by the post office and reportedly left near or outside the office door. The security guard then became suspicious either based on the way it was left behind or because of the writing on the package.
Source:
http://www.monroenews.com/apps/pbcs.dll/article?AID=/20080107/NEWS01/232694066

[Return to top]

Agriculture and Food Sector

18. *January 8, Associated Press* – (Massachusetts) **Third man dies after drinking tainted milk.** An 87-year-old man was the third person to die from a deadly bacteria outbreak triggered by consuming tainted milk products from Whittier Farms, a central Massachusetts dairy, the state health department said Monday. Health officials say the bacteria entered the dairy's milk supply after it was pasteurized. The number of people sickened by listeria bacteria also rose to five after health officials linked a 31-year-old Middlesex County woman diagnosed in September with listeriosis to products from the diary. Two of those victims died in June and October. Another elderly man and a pregnant woman survived, although the woman miscarried. Managers of the family owned dairy, which remains closed, have said in a statement that they were "extremely concerned about the situation and will be working to obtain the results of the investigation."
    Source: http://www.thebostonchannel.com/health/14997222/detail.html

19. *January 7, Star Press* – (Indiana) **Local counties named drought disaster areas.** Delaware, Blackford, and Henry counties are among 74 Indiana counties named recently as primary natural disaster areas because of losses caused by extended drought conditions that occurred June 5 – November 7, 2007. All qualified farm operators in the designated areas are eligible for low interest emergency loans from U.S. Department of Agriculture's Farm Service Agency, provided eligibility requirements are met. The USDA has also made other programs available to assist farmers and ranchers, including the Emergency Conservation Program, Federal Crop Insurance, and the Noninsured Crop Disaster Assistance Program.
    Source: http://www.thestarpress.com/apps/pbcs.dll/article?AID=/20080107/NEWS01/801070333/1002

20. *January 7, U.S. Cattlemen's Association* – (National) **U.S. Cattlemen to Congress: Fix USDA's Argentina mess.** A year ago, the U.S. Department of Agriculture issued a little-known and little-publicized proposal to import beef from Argentina, despite the country's repeated problems with foot and mouth disease (FMD). The U.S. Cattlemen's Association (USCA) has made blocking the USDA's action one of its top priorities in 2008.Under the USDA proposal, beef and cattle imports would be allowed from areas of Argentina that are considered to be FMD free. USCA says enforcing such a plan would be impossible and shipments containing FMD would likely slip through the cracks. USCA is calling on all U.S. livestock producers to get involved to defeat the USDA's proposal. Other groups are following USCA's lead on the issue. Numerous state cattle organizations have sent letters to Congress and the USDA opposing the proposed policy and have passed resolutions against regionalized trade with Argentina.
    Source: http://www.cattlenetwork.com/content.asp?contentid=188159

[Return to top]

Water Sector

21. *January 7, Associated Press* – (California) **California Senate leader says he will delay his proposed water bond.** The California state Senate leader on Monday said he will

not push a water bond proposal this year because of the state's budget crisis. He was promoting a $6.8 billion initiative to fund water recycling, conservation, and environmental cleanup, but he said such spending should be delayed now that the state is facing a budget shortfall projected at $14 billion over the next 18 months. He also asked the California Chamber of Commerce and farmers to delay their competing $11.7 billion water bond initiative, which they want to put before voters in November. A mild winter in 2007 and a federal court order restricting pumping from the Sacramento-San Joaquin Delta prompted California's governor to call for a special legislative session late last year. He wanted lawmakers to create a long-term water plan for storing, moving and conserving water, but Democrats and Republicans failed to agree. The Senate leader urged the governor to allocate $611 million from three water-related initiatives previously approved by voters: propositions 1E and 84, approved in 2006; and Proposition 13, passed in 2000. The Senate leader wants to use the money for flood control, cleaning up groundwater sources, improving drinking water, protecting the delta, and other projects.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/01/07/financial/f170346S72.DTL&type=politics

22. *January 7, Star Tribune* – (Minnesota) **Ridding landfill of oozing 3M chemicals will be costly, lengthy.** It could take Minnesota up to five years to keep PFBA, a coatings compound used in photographic films and other products that was dumped legally in a landfill three decades ago by 3M, from oozing out of the former Washington County landfill into the groundwater in Lake Elmo, state pollution control officials said Monday. The cost is now estimated at $27.6 million, which would make it the most expensive such effort under the state landfill remediation program. That plan would unearth 35 acres of waste and put it in a new leak-proof landfill on the site. It is considered the best option to halt the release of 3M chemicals buried amid the garbage, according to a consultant's assessment presented Monday to Lake Elmo residents Chemicals from the landfill and another company-owned closed dump in Oakdale have turned up in 387 private wells in the area, according to the Minnesota Department of Health. About 200 homes have been shifted to city water service, and others have had filter systems installed.
Source: http://www.startribune.com/local/east/13516126.html

23. *January 7, Arizona Daily Star*– (Arizona) **Green Valley plant aims to clean up drinking water.** A Canadian company that specializes in the treatment of industrially contaminated water is working on a pilot plant to remove sulfate contamination coming from the Sierrita Mine northwest of Green Valley, Arizona. The plant, which will be built this year and start running by 2009, will be the first large-scale operation to use the company's ion-exchange process for removing sulfates from groundwater. Authorities have known since the mid-1980s that sulfates seeping from the Sierrita Mine had polluted groundwater and represented a potential threat to drinking-water supplies. In 2005, the Community Water Co. of Green Valley had to close two drinking-water wells that had sulfates at levels above 500 parts per million, more than twice the recommended level. According to a press release from BioteQ Environmental Technologies, the two companies will work together to design, build, and operate the

demonstration plant. Freeport-McMoRan, the owner of the mine, will pay for the construction and operation, and BioteQ will license the technology to the mining company so it can be used at other sites if the technology works. The plant will be able to treat 125 gallons per minute. The company said the ion-exchange method for removing sulfates from water is less expensive than reverse osmosis, and its only byproduct is gypsum, which is used in making building products and fertilizers.
Source: http://www.azstarnet.com/metro/219363

24. *January 6, KSWO 7 Lawton* – (Oklahoma) **Fish habitat dying in Medicine Park due to chlorine leak.** Reports say a chlorine leak from the Lawton Water Treatment Plant made the creek water so toxic, all the underwater wildlife is expected to die. The mayor of Medicine Park, Oklahoma, says it has been a problem since the middle of last week. On Sunday, the leak was fixed, but not soon enough to save the fish. The mayor says the leak at the plant sent so much chlorine downstream it was more than 200 times the allowed limit. Once the leak is fixed, the mayor of Medicine Park hopes the City of Lawton will pay to replace the fish. The plant has pumped the water out of that tank for now, and they will meet tomorrow to discuss a permanent fix.
Source: http://www.kswo.com/Global/story.asp?S=7585444

[Return to top]

Public Health and Healthcare Sector

25. *January 8, Washington Post* – (Maryland) **Severe dearth of doctors forecast for Maryland.** Much of Maryland faces a doctor shortage that could become severe by 2015, forcing patients to wait longer for appointments, search for specialists, and turn more frequently to emergency rooms for help, according to a report released yesterday. Southern Maryland is expected to be hit hardest -- the region lacks physicians in most categories now -- with Western Maryland and the Eastern Shore close behind. With nearly one in three specialists older than 60, Montgomery and Prince George's counties will confront a surge of retirements. The two jurisdictions already count fewer general surgery physicians and residents per 100,000 people than any area in the state, but Southern Maryland. The report by two state health-care groups says the impact will be felt most acutely in overextended emergency rooms, where finding specialists for on-call duty is difficult today. It urges medical and elected leaders to take "bold steps" to attract and keep clinicians, but includes no price tag for nearly a dozen suggested actions, including higher physician fees and incentives to draw doctors to rural areas. The issues are not confined to Maryland. A Northern Virginia alliance of hospitals and colleges is halfway through a four-year initiative to increase the ranks of nurses and other health-care workers and fill thousands of positions that by 2020 are projected to go wanting without action. By that same year, the American Medical Association foresees a national shortfall of 20,000 doctors. Cities with academic medical centers, such as the District of Colombia, will probably fare better.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/01/07/AR2008010701909.html

26. *January 8, Citizen of Laconia* – (New Hampshire) **Outbreak of virus triggers**

precautions. In New Hampshire, two of the senior wings at Lakes Region General Hospital (LRGH) have been closed to new admissions and visitors due to a minor outbreak of a gastrointestinal virus. LRGH is the latest medical care facility to be struck by such a problem and staff at the St. Francis Rehabilitation and Nursing Center continue to deal with an outbreak of norovirus. The LRGHealthcare Chief of Staff said hospital officials have sent samples of the virus to the state's Department of Health and Human Services, as is standard procedure when such an ailment strikes a nursing home, virus, or school. He said such ailments are common and present less of a problem for those contracting them in isolation, but he said the ailments can present a major challenge for those dealing with large amounts of people, especially the elderly, in a confined area because of the ailments' ability to spread quickly.
Source:
http://www.citizen.com/apps/pbcs.dll/article?AID=/20080108/GJNEWS02/447404591/-1/CITIZEN

Government Facilities Sector

27. *January 7, WKMG 6 Orlando* – (Florida) **Entire military tank, bombs found buried near Central Florida school.** Workers, who found and detonated more than 400 pounds of World War II-era bombs and munitions near a Central Florida middle school, have discovered an entire military tank buried underground near the campus. U.S. Army Corps of Engineers said about 50 23-pound bombs, several rockets, a rocket booster, and a cannon have been found buried near Odyssey Middle School since December 27. Part of the school grounds was used by the Army in the 1940s to train bombardiers for combat. Three small areas on school grounds still have to be checked for munitions. School leaders and the Army officials said children at the school are safe.
Source: http://www.local6.com/news/14992012/detail.html

[Return to top]

Emergency Services Sector

28. *January 7, RCR Wireless News* – (National) **Industry delay could impede emergency-alert initiatives.** The Federal Communications Commission boasts that its new wireless emergency-alert proposal will help fulfill its statutory charter to promote the safety of life and property, but the agency's head conceded to lawmakers that there is no assurance that warnings of terrorist threats or natural disasters will actually be delivered to the nation's 250 million cellphone subscribers. "By starting this rulemaking today, we take a significant step towards implementing one of our highest priorities — to ensure that all Americans have the capability to receive timely and accurate alerts, warnings and critical information regarding impending disasters and other emergencies irrespective of what communications technologies they use," stated the FCC in its 118-page mobile alert plan. The current emergency-alert system dates back to the Cold War, and relies largely on broadcast TV and radio. The terrorist attacks of September 11, 2001, prompted Congress to re-examine the country's emergency warning regime.

Source: http://www.rcrnews.com/apps/pbcs.dll/article?AID=/20080107/SUB/302784303/1020/FREE

29. *January 7, American Red Cross* – (National) **Companies getting into business of disaster relief.** A Red Cross initiative, Ready When the Time Comes (RWTC), recruits volunteer teams from local businesses and trains them in emergency response to ensure their communities are prepared for emergencies and able to rebuild quickly after disasters strike. Through RWTC, businesses partner with the Red Cross, thereby enabling their employees to receive free training in disaster relief functions. In return, corporate partners commit to making their trained employees available for disaster service. Thus far, eight Red Cross chapters have launched pilot RWTC programs, training more than 2,500 new disaster response volunteers from 80-plus partner organizations. The chapter in New York will launch its pilot program on January 28; launches at seven other chapters are scheduled for later this year.
Source: http://www.redcross.org/article/0,1072,0_312_7419,00.html

[Return to top]

Information Technology

30. *January 8, Register* – (National) **Hackers turn Cleveland into malware server.** Tens of thousands of websites belonging to Fortune 500 corporations, state government agencies, and schools have been infected with malicious code that attempts to engage in click fraud and steal online game credentials from people who visit the destinations, security researches say. More than 94,000 URLs had been infected by the fast-moving exploit, which redirects users to the uc8010-dot-com domain. The security company Computer Associates was infected at one point, as were sites belonging to the state of Virginia, the city of Cleveland, and Boston University. Malicious hackers were able to breach the sites by exploiting un-patched SQL injection vulnerabilities that resided on the servers, according to the CTO for the SANS Internet Storm Center. The injections included javascript that redirected end users to the rogue site, which then attempted to exploit multiple vulnerabilities to install key-logging software that stole passwords for various online games. According to a researcher for ScanSafe, the exploits forced end users to visit sites that pay third parties a fee in exchange for sending them traffic. She speculates the attackers signed up as affiliates of the sites and then profited each time an end user was infected. The malware also installed keyloggers on end user machines that stole passwords to various online games, another researcher said. He added that the uc8010-dot-com domain was registered in late December using a Chinese-based registrar, indicating the attackers were fluent in Chinese.
Source: http://www.theregister.co.uk/2008/01/08/malicious_website_redirectors/

31. *January 7, IDG News Service* – (National) **U.S. government needs new cybersecurity steps, Symantec warns.** U.S. government agencies need to take additional steps to protect against cybersecurity problems after a series of congressional hearings and reports exposed several weaknesses in 2007, representatives of Symantec Corp. said. The government sector, including state and local governments, accounted for 26 percent

of data breaches that could lead to identity theft in the first half of 2007, according to Symantec's latest Government Internet Security Threat Report, published in September. The U.S. Government Accountability Office (GAO) also issued about a dozen reports in the last six months criticizing federal agencies for not fully implementing the GAO's cybersecurity recommendations. While U.S. agencies have a set of cybersecurity rules set out in the Federal Information Security Management Act, agencies are not held accountable when they have breaches, said Symantec's vice president for the public sector. Agencies do not lose funding from Congress after cybersecurity incidents, he said. Agencies can take more steps to fix problems, he added, such as to inventory IT assets, to develop comprehensive cybersecurity plans, do systematic vulnerability testing, have a data backup plan and back up frequently. There still seems to be interest from lawmakers in agency cybersecurity and breach notification, he said. The hearings and information requests from lawmakers are bringing to light multiple attacks and breaches at agencies, he said. "There's no real mechanism requiring agencies to report breaches," added Symantec's federal government relations manager.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9056002&taxonomyId=17&intsrc=kc_top

32. *January 7, Computerworld* – (National) **'Hacker safe' Web site gets hit by hacker.** On Friday, Geeks.com, a $150 million company specializing in the sale of computer-related excess inventory and manufacturers' closeouts, began notifying an unspecified number of customers whose personal and financial data may have been compromised by an intrusion into the systems that run the online technology retailer's Web site. The compromised information included the names, addresses, telephone numbers, and Visa credit card numbers of customers who had shopped at Geeks.com, according to a copy of the letter that was posted on The Consumerist blog. Its Web site prominently proclaims that it is tested on a daily basis by ScanAlert Inc., a vendor in Santa Clara, California, that agreed in October to be acquired by McAfee Inc. McAfee officials were not immediately available to comment on what might have happened at Geeks.com. A telephone operator at Geeks.com's headquarters in Oceanside, California, said that she was unable to find anyone at the retailer who could comment about the incident. Last week's notification included a number for non-U.S. residents to call, suggesting that the breach may have affected customers in other countries as well. According to a letter, which was signed by chief of security at Geeks.com, the intrusion has been reported to local law enforcement authorities, as well as to the U.S. Secret Service. The incident has also been reported to Visa without providing any indication of why only Visa card numbers appear to have been compromised.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9056004&source=rss_topic17

33. *January 7, Network World* – (International) **Nugache worm kicking up a storm.** Although the infamous Storm worm enters 2008 with a reputation as the world's most dangerous botnet, security experts say there is an up-and-comer called Nugache. Nugache was first sighted about two years ago, but last month, hackers, believed to be

tied to the notorious Russian Business Network online criminal mob, gave Nugache a facelift, copying many of the successful attributes of Storm, such as encryption, a rootkit, and the ability to spread as Web-borne malware. "Nugache now includes the ability to encrypt itself and every version that rolls out is generated a bit differently to obfuscate detection," said the vice president of technology evangelism at Secure Computing. Nugache is now also peer-to-peer controlled to put it under a more decentralized command-and-control structure that makes it difficult to take down the botnet it can construct once it infects desktop machines. The rise of the Nugache botnet appears to already be giving the Storm botnet more competition. Prices as low as 1 million spam messages for $100 are being advertised online mainly because of the rise of Nugache, said the researcher. Business and consumers should be aware that Nugache could attempt to compromise their desktop machines in various ways, particularly through Web-based drive-by downloads. One way it has been seen spreading is through URLs embedded by attackers in blogs. "They will create the blog entry, then embed hundreds of key words and embed pointers to other blog entries, such as the second blog entry pointing back to the first entry," he said. "Google rates you on how many other people point to your URL. So they're getting down the science of artificially inflating their position in the search engine. They want these blog postings to show up on the top."
Source: http://www.networkworld.com/news/2008/010708-nugache-worm.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

34. *January 7, RCR Wireless News* – (National) **Industry challenges FCC's emergency backup power rule.** The Federal Communications Commission (FCC) is facing a gathering legal storm over its emergency back-up power rule. The new rule, among other things, calls for a minimum 24 hours of emergency back-up power for telecom assets inside central offices and eight hours for other facilities such as cell sites, remote switches, and digital loop carrier system remote terminals. "The FCC lacks authority to issue the rule," Sprint Nextel told the U.S. Court of Appeals for the District of Columbia Circuit. "There is no provision in the Communications Act directing the commission to issue regulations requiring wireless carriers to adopt back-up power rules, and the commission's attempt to rely on 'ancillary jurisdiction' … strains the reach of those provisions beyond the breaking point." Cellphone industry associations CTIA and USA Mobility Inc., whose appeals of the back-up power rule have been consolidated, told the court expedited treatment of the appeal is justified because the back-up power rule "would impose overwhelming compliance costs, most of which would be incurred

during the pendency of these cases." The two parties also pointed to the FCC's own admission that compliance with the back-up power rule could force carriers to take down cell sites critical to wireless communications, including emergency 911 services. The FCC told the court it does not oppose expedited treatment of back-up power appeal, but would vigorously oppose Sprint Nextel's stay motion.
Source:
http://www.rcrnews.com/apps/pbcs.dll/article?AID=/20080107/SUB/3392962/1005/allnews

35. *January 6, Chicago Tribune* – (National) **Workers' remote wireless access to documents lets hackers grab data.** Smart phones are poised to become the next major security challenge for businesses. Consumer-oriented mobile phones, which have far fewer safety features, are increasingly taking on such PC-like characteristics as Wi-Fi connectivity, making them attractive to people who want to use them for work. In a Computing Technology Industry Association survey conducted this year of 1,070 small businesses in North America, 60 percent of firms said they have seen an increase in the past year in security issues related to the use of handheld computing devices. A specialist at Alternative Technology said the concern for businesses is whether these phones "will cause so much of a risk that they will eventually ... just be banned from corporate environments." The increasing ease of working remotely is creating a growing set of security concerns for companies. So far, there have not been any high-profile epidemics of mobile viruses like the "I love you" worm for PCs that spread rapidly around the world in 2000. But developers have demonstrated the destructive potential of such worms. The "Cabir" virus, which first appeared in 2004, used Bluetooth technology to jump from phone to phone. Another virus, known as "Commwarrior.A," replicated itself by sending a picture or text message to people in the infected device's contacts list. Theft is a bigger issue now. While hacking once was about bragging rights or cyber vandalism, security industry officials say profit now largely drives attacks, as the kind of information traveling over wireless networks grows in volume and value.
Source:
http://www.freep.com/apps/pbcs.dll/article?AID=/20080106/BUSINESS07/801060605/1020

[Return to top]

Commercial Facilities Sector

36. *January 8, WQAD 8 Davenport* – (Illinois; Missouri) **Tornados rip through the Midwest.** Tornados leveled four of his historic buildings and damaged six others in Northern Illinois. Meanwhile in southwestern Missouri, tornados killed two and injured six. Dozens of homes and businesses are damaged and power lines are down there.
Source: http://www.wqad.com/Global/story.asp?S=7592110&nav=1sW7

37. *January 6, Scripps Treasure Coast Newspapers* – (Florida) **Explosive devices located, blown up in Indian River County.** An off-duty sheriff's deputy Sunday afternoon ran over an explosive device that was so powerful it jolted her 8,600-pound sport utility vehicle. And upon further inspection, three more suspicious devices were found

prompting officials to shut down the road and request one family consider evacuating their home. The Indian River County Fire Rescue and the St. Lucie County bomb squad, along with its new $164,000 high-tech robot and $258,000 bomb disposal truck, responded to the scene, where bomb technicians blew up the devices with a 12-gauge water cannon.
Source: http://www.tcpalm.com/news/2008/jan/06/30explosive-devices-located-blown-up/

[Return to top]

National Monuments & Icons Sector

38. *January 7, Daily Sentinel* – (Utah) **Tar sand development may hurt parks.** Tar sands development could severely affect Utah's Canyonlands National Park, Glen Canyon National Recreation Area, and a stretch of the San Rafael Swell along Interstate 70, according to a Bureau of Land Management report. The 1,400-page government report, called the Oil Shale and Tar Sands Draft Programmatic Environmental Impact Statement, was released in December and outlines the landscape-altering changes that could occur when the BLM's congressionally mandated commercial oil shale and tar sands leasing program for Utah, Colorado, and Wyoming begins. If the BLM's preferred tar sands development scenario goes forth, more than 100,000 acres of wilderness-quality land could be industrialized, construction of reservoirs would alter natural streamflow patterns, hydrocarbons and herbicides could cause "chronic or acute toxicity" in wildlife, and habitat for 20 threatened or endangered species could be lost, the report says.
Source: http://www.gjsentinel.com/hp/content/news/stories/2008/01/07/010808_1b_Tar_Sands.html

[Return to top]

Dams Sector

39. *January 8, Caspar Star Tribune* – (Wyoming) **Dam report to get airing by legislative panel.** The Green River Basin in western Wyoming is one of the few areas left in Wyoming that has water to develop and land needed to build dams and reservoirs. Water officials believe more storage is needed, particularly for irrigators in the basin and for towns and communities that are growing due to the natural-gas boom. The state has been searching for decades for just the right spot to build a dam across the Upper Green River. The Wyoming Water Development Commission presented a report to the Legislature's Select Water Committee in September that looked at the pros and cons of building what is known as the Kendall dam. The commission will decide whether to hold a public hearing on that report, when the commission meets on Wednesday. Past reports have shown that damming the river could provide irrigation water for about 71,000 acres and provide much-needed water during drought. The most recent commission report said it would take lots of time, money and a hard-to-get federal construction permit from the U.S. Army Corps of Engineers to complete the Kendall

dam and reservoir project.
Source: http://www.billingsgazette.net/articles/2008/01/08/news/wyoming/25-damreport.txt

[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