Homeland Security

Daily Open Source Infrastructure Report for 27 January 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- According to the Christian Science Monitor, at least three U.S. oil companies were the target of a series of previously undisclosed cyberattacks, which occurred in 2008. The breaches were focused on valuable "bid data" detailing the quantity, value, and location of oil discoveries worldwide. (See item **3**)
- The Associated Press reports that authorities in Branchburg, New Jersey on Monday seized a cache of weapons and ammunition from the motel room of a Navy veteran from Reston, Virginia, who also had maps of a U.S. military facility and a town in another state. (See item **28**)

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. *January 26, WRC 4 Washington and Associated Press* – (Maryland) **Driver seriously injured in apparent manhole explosion.** An investigation into the source of an unidentified odor in Montgomery County closed a stretch of Georgia Avenue. Authorities investigating an accident in Wheaton reported a strange odor Monday

afternoon, a Montgomery County Fire Department spokesman said. At least one manhole cover in the area was not in its original position, he said. Police who noticed the smell were investigating an apparent manhole explosion that sent a manhole cover through the windshield of an SUV, striking the driver in the face before landing in the backseat, a News4 reporter said. She is expected to survive. Hazmat crews worked with Pepco and Washington Gas to try to identify the odor, which might be a gas leak. As a precaution, officials evacuated townhouses, apartments and a church in the area. About 75 others were told to stay inside. One person who smelled the odor and felt sick is being evaluated. Georgia Avenue was closed between University Boulevard and Dennis Avenue, but two lanes in each direction had reopened by about 6 p.m.
Source: http://www.nbcwashington.com/news/local-beat/Woman-Seriously-Injured-in-Apparent-Manhole-Explosion-82623817.html

2. *January 26, Tank Storage Magazine* – (Oklahoma) **Blueknight storage tank hit by lightning.** On 20 January, a fire at Blueknight Partners' oil storage tanks in Cushing, Oklahoma, burned for eight hours until it was finally put out. Although the company's operations were not halted, 1,000 barrels of the 55,000-barrel storage tank of crude oil were destroyed after the tank was struck by lightning and a fire broke out. The storage tank sustained minor damage but is still all in one piece. There are no signs of any damage to the environment and no one was injured. The Cushing Fire Chief explained that the fire would have been much worse if the tank had not been filled to the top with oil, as the full tanks allowed for no air between the oil and the lid. The spokesman for Blueknight Energy Partners said, "We will conduct an internal assessment to determine the extent of the damage to the tank, which appears to have been limited to the seal encircling the top."
Source: http://www.tankstoragemag.com/industry_news.php?item_id=1674

3. *January 25, Christian Science Monitor* – (National) **U.S. oil industry hit by cyberattacks: Was China involved?** At least three U.S. oil companies were the target of a series of previously undisclosed cyberattacks that may have originated in China and that experts say highlight a new level of sophistication in Internet espionage. The oil and gas industry breaches were focused on valuable "bid data" detailing the quantity, value, and location of oil discoveries worldwide, sources familiar with the attacks say and documents obtained by the Monitor show. The companies — Marathon Oil, ExxonMobil, and ConocoPhillips — did not realize the full extent of the attacks, which occurred in 2008, until the FBI alerted them that year and in early 2009. Federal officials told the companies proprietary information had been flowing out, including to computers overseas, a source familiar with the attacks says and documents show. The data included e-mail passwords, messages, and other information tied to executives with access to proprietary exploration and discovery information, the source says. While China's involvement in the attacks is far from certain, at least some data was detected flowing from one oil company computer to a computer in China, a document indicates. Neither Marathon Oil, ExxonMobil, nor ConocoPhillips would comment on the attacks or confirm that they had happened. But the breaches, which left dozens of computers and their data vulnerable in those companies' global networks, were confirmed over a five-month Monitor investigation in interviews with dozens of oil

industry insiders, cybersecurity experts, former government officials, and by documents describing the attacks. The attacks penetrated the companies' electronic defenses using a combination of fake e-mails and customized spyware programs to target specific data, according to multiple sources and documents.
Source: http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved

[Return to top]

Chemical Industry Sector

4. *January 26, McClatchy Tribune and Houston Chronicle* – (Texas) **Sulfuric acid tanker among derailed cars.** Union Pacific brought in heavy equipment on Janaury 25 to remove eight cars that had derailed in Baytown, including one filled with sulfuric acid and another with antifreeze, authorities said. Baytown's hazardous materials team inspected the cars that tumbled from the track about 12:20 a.m. on the north side of the Coady railroad yard and found no leaks, said Baytown's assistant fire chief. The cause of the mishap remains under investigation, railroad officials said. The train that slid from the track services the petrochemical industry in the Baytown area. Two of the eight derailed cars were transporting potentially hazardous and the rest contained "some various residues," he said. No injuries were reported.
Source: http://www.tradingmarkets.com/news/stock-alert/unp_brief-sulfuric-acid-tanker-among-derailed-cars-726633.html

5. *January 26, West Virginia Public Broadcasting* – (West Virginia) **Chemical Safety Board investigates DuPont plant.** Three chemical leaks at DuPont's Belle plant near Charleston last week have left one employee dead and the plant temporarily closed for closer inspection. Several agencies are now investigating what happened at the chemical factory. A West Virginia congresswoman was waiting to be briefed by DuPont officials the evening of January 25. She said she is glad to see the company reacting. DuPont decided to temporarily stop production at the plant while its evaluating operating procedures. "There's a good history in that plant in being incident free, but it's troublesome when you hear three leaks in that many days; I think that's a huge red flag," she said. The Chemical Safety Board (CSB) announced on January 25 afternoon that it will investigate the leaks and is sending a four-member team to the plant. The CSB says it is aware of six other leaks at the plant since 2006. Representatives from the Occupational Safety and Health Administration and the West Virginia Department of Environmental Protection (DEP) were at the plant on January 25. A DEP spokeswoman says the DEP oversees air quality, water quality and hazardous waste permits for the plant and regularly inspects the plant. DuPont issued a press release Monday stating that man died on January 24 after being exposed to a toxic chemical used to make plastics and pesticides. The chemical leaked out of a transfer hose.
Source: http://www.wvpubcast.org/newsarticle.aspx?id=12900

[Return to top]

Nuclear Reactors, Materials and Waste Sector

6. *January 22, WSJM 94.9 Benton Harbor* – (Michigan) **Palisades nuclear plant cited for low-level safety violation.** The Palisades nuclear power plant was sanctioned this month by the Nuclear Regulatory Commission for violating safety standards regarding spent fuel rods. An NRC spokeswoman says that the Covert facility was cited for problems with the material in which it was storing the rods. A certain amount of boron carbide is supposed to be used in the spent fuel pool to prevent a nuclear reaction from occurring there. The NRC spokeswoman says that it was a relatively low-level safety violation. She stated that Palisades was not fined, and no one was ever in danger. The NRC will continue to monitor the spent fuel rod pool while the plant determines what caused the problem in the first place.
Source: http://www.wsjm.com/Palisades-Nuclear-Plant-Cited-For-Low-Level-Safety/6184219

[Return to top]

Critical Manufacturing Sector

7. *January 26, Justice News Flash* – (National) **Recall: Thermador built-in ovens pose a fire hazard.** Announced by the U.S. Consumer Product Safety Commission (CPSC), BSH Home Appliances Corp. have voluntarily recalled Thermador built-in ovens after discovering a fire hazard. The recall was announced on Thursday, January 21, 2010. BSH Home Appliances Corp. has recalled nearly 37,000 more built-in ovens after they previously recalled 42,000 in June 2007. The ovens reportedly can have gaps in the insulation, which can cause overheating when used in the self-cleaning model, posing a fire hazard. There have been three reports of incidents, in which two resulted in fires that damaged nearby cabinetry. No injuries have been reported. The recall involves Thermador brand built-in double ovens with model numbers C272B, C302B, SEC272, SEC302, SECD272, and SECD302 and serial numbers between FD8403 through FD8701, which can be found on the underside of the control panel. The recalled products were sold at appliance and specialty stores across the country from June 2004 through July 2007 for between $3,000 and $4,400. Consumers are advised to discontinue use of the self-cleaning mode immediately, and contact BSH Home Appliances Corp. to schedule an inspection and free repair, if necessary. For additional information, consumers are instructed to contact Thermador.
Source: http://www.justicenewsflash.com/2010/01/26/recall-thermador-builtin-ovens-pose-fire-hazard_201001263112.html

8. *January 26, Reliable Plant Magazine* – (Mississippi) **Mueller Industries cited for 128 OSHA violations.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) on January 25 issued three Mueller Industries Inc. subsidiaries in Fulton, Mississippi, 128 citations for allegedly exposing workers to safety and health hazards. OSHA began its investigation in July 2009 after a maintenance worker employed by Mueller Copper Tube Company Inc., a subsidiary of Mueller Industries, was killed, and two other workers were injured when naphtha, a flammable liquid of

hydrocarbon mixtures, leaked from an electric pump and ignited. "Mueller Industries subsidiaries' dangerous practices exposed workers at their facilities to a variety of hazards that ultimately took one worker's life," said the assistant secretary of labor for OSHA. Mueller Industries is fined $683,000.
Source: http://www.reliableplant.com/Read/22431/Mueller-Industries-OSHA-violations

[Return to top]

Defense Industrial Base Sector

9. *January 26, Global Security Newswire* – (Tennessee) **New HEU storage site OK'd to open.** The U.S. National Nuclear Security Administration said Monday it had given the final go-ahead to begin the transfer of highly enriched uranium to a new, high-security storage facility at the Y-12 National Security Complex in Oak Ridge, Tennessee. Much of Y-12's weapon-grade material is set to be moved to the $549 million Highly Enriched Uranium Materials Facility within 90 days, saving roughly $26 million in security dollars on a transfer operation originally expected to last roughly 13 months. The storage site was intended to reduce costs and improve the efficiency of securing and maintaining the uranium, which could be used in U.S. nuclear weapons and, through a conversion process, as fuel for reactors used in research, production of medical isotopes, and other activities.
Source: http://www.globalsecuritynewswire.org/gsn/nw_20100126_9123.php

10. *January 25, Military Times* – (National) **Navy, Northrop working on faulty welds.** The Navy's top civilian acquisition official said he was confident in shipbuilder Northrop Grumman's "commitment to delivering quality ships to the Navy" even after the Navy announced last week that all Northrop's warships built on the Gulf Coast were being re-inspected for faulty welds. "In the rare instance where an issue like this arises, the Navy and industry have always worked together toward a quick and effective resolution. This remains the case today," said the assistant secretary of the Navy for research, development and acquisition, in a statement released Monday. "At no time did the weaknesses that were discovered endanger the safety of the crews, and the Navy has determined that existing welds are satisfactory for current ship operation. We have worked hard to ensure all ships meet or exceed fleet standards, and are reliable and combat ready assets. Plans are in place for inspections and required repairs to all affected ships during their normal industrial availabilities, with many already in progress." His statement was the first public comment from the Navy Department's leadership on the January 21 announcement by Naval Sea Systems Command about the weld problems. Still, the statement did not answer the pressing questions raised by NavSea's announcement: How many warships — including destroyers and small- and large-deck amphibs — are potentially affected by the faulty welds? How or why did Navy inspectors sign off on out-of-spec welds that were discovered later on? How many of Northrop's welders and inspectors, and Navy inspectors, had to be decertified and recertified to work on ships after the problems were discovered? Who will pay for repairs?

Source:
http://www.militarytimes.com/news/2010/01/navy_stackley_statement_012510w/

11. *January 22, WREX 13 Rockford* – (Illinois) **Complaint filed against NDK for plant explosion.** A complaint alleging environmental violations against NDK Crystal, Inc. has been filed. The complaint says various hazardous materials were released into the air after the blast on December 7, 2009. A 63-year-old truck driver from Chesterton, Indiana, was killed in the incident. He was hit by flying debris while pumping gas at the nearby Belvidere Oasis off of Interstate 90. Along with the complaint, the Boone County state's attorney and the Illinois attorney general have filed a motion to shut down NDK until the investigation into the cause of the deadly blast is concluded. "The force of this explosion had tragic consequences for an innocent bystander and resulted in the release of several potentially hazardous materials. Before we can ensure that the plant can be operated safely in the future, we must know why the explosion happened," the attorney general said. NDK makes crystals used in computers, telephones, liquid crystal displays and other electronics. A hearing on the complaint is scheduled for March 19.
Source: http://www.wrex.com/Global/story.asp?S=11866379

[Return to top]

Banking and Finance Sector

12. *January 25, QMI Agency* – (Florida; International) **Ponzi scam alleged in billions.** The Ponzi scheme allegedly orchestrated by two Calgary businessmen, initially suspected of involving up to $400 million, could be as high as $5 billion, a Florida court has been told. In a draft order presented by a bankruptcy trustee lawyer, it is suggested the scheme is much larger than initially thought. The lawyer, based on evidence from a forensic auditor, said a southern district of Florida judge should rule the two Calgarians collected massive investments. The lawyer, in his 40-page draft obtained Friday by the Sun, said three-quarters of those who poured money into the two defendants interests were Canadian investors. The lawyer said the defendant collected investments in a variety of Miami-based Merendon subsidiaries and co-mingled the funds.
Source: http://cnews.canoe.ca/CNEWS/Crime/2010/01/22/12585276-qmi.html

13. *January 25, International Falls Daily Journal* – (Minnesota) **Officals warn about phone scam regarding credit cards.** A number of International Falls area residents have received fraudulent calls since January 21 as a part of a nationwide scam apparently based on compromised cell phone information. An International Falls Police Investigator said on January 22 that a block of telephone numbers with the 240 prefix and the 218 area code have been targeted by a someone who is "vishing." In this case, the automated voice calling indicates there may be a problem with a credit or check card and says that the only way to deactivate the card is by entering into the telephone their account numbers. The scam artists are attempting to make the calls sound local, the investigator said. According to TruStar Federal Credit Union, members are being directed to ignore computer-voiced messages asking them to enter personal

identification to “activate” or “confirm” their debit card or ATM cards. The computer voice has referred to the local financial institution variously as “TriStar,” or “Trust-star,” in addition to the actual name of the credit union.
Source: http://www.ifallsdailyjournal.com/news/police-reports/officals-warn-about-phone-scam-regarding-credit-cards-laurel-beager-editor-101

[Return to top]

Transportation Sector

14. *January 26, HawaiiNewsNow* – (National) **Ship loses cargo after violent storm.** Six containers were lost at sea after a Horizon Lines cargo ship plowed through a violent storm on its way to Honolulu. On Monday night, workers were off-loading what was left. The U.S. Coast Guard said pollution investigators were out at Pier 1 where the Horizon Hunter is docked. Crews brought out a crane to lift the damaged cargo off of the ship. “Several containers stowed above deck sustained varying degrees of damage,” said a spokesperson for Horizon Lines. “The crew is safe now, and uninjured.” Sky News Now was above. The ship, docked at Honolulu Harbor, came from Los Angeles, bound for Guam. There is no word yet on what was inside the lost containers. For now, removing the damaged containers safely is the company’s top priority. The U.S. Coast Guard says the items inside the damaged containers include food, cleaners, and cars. As of Monday night, the Coast Guard said investigators did not find any pollutants coming out of the damaged cargo.
Source: http://www.hawaiinewsnow.com/Global/story.asp?S=11879947

15. *January 26, CNN* – (National) **New rule for truck, bus drivers: No texting.** Drivers of commercial trucks and buses are prohibited from texting under federal guidelines that the U.S. Transportation Secretary announced Tuesday. The prohibition is effective immediately. Truck and bus drivers who text while driving commercial vehicles may be subject to civil or criminal penalties of up to $2,750, the Department of Transportation said in a news release. The release did not offer specifics on how the prohibition will be enforced. One of the nation’s largest groups representing professional truck drivers — the Owner-Operator Independent Drivers Association — expressed support for the goal but dismay at its implementation. “We support where they are going, but not how they got there,” said the group’s executive vice president. “Making their action effective immediately bypasses normal regulatory rulemaking processes. Those processes allow actions to be vetted for unintended consequences as well as potential implementation and enforcement problems. The U.S. President also signed an executive order requiring federal employees not to text while driving government-owned vehicles or with government-owned equipment, and were ordered to comply with the move December 30.
Source: http://www.cnn.com/2010/POLITICS/01/26/trucks.texting.ban/?hpt=T1

16. *January 26, Associated Press* – (Maryland) **2 workers for Metro rail line hit, killed on Md. track in latest in string of fatalities.** Two veteran Metro workers were struck and killed by a maintenance truck on a track Tuesday, the latest in a string of fatalities

since last year in the Washington area's transit system. The men were installing safety equipment on a track that was closed to regular service for the night when they were hit. One of them died at the scene, a few blocks from the Rockville Metro Station, and the other on the way to a hospital. Metro says both men were automatic train control technicians. They were hit by a large truck equipped to drive on the track when electricity is shut down. The National Transportation Safety Board has launched an investigation into the accident. The accident disrupted the morning rush for many commuters from Maryland as red line service was shut down between the Shady Grove and Twinbrook stations while the crash was investigated. Shuttle service was being provided between the stations. The employees who were killed were installing new automatic train control equipment in the track bed. A Metro spokesman said the work being done Tuesday morning was routine maintenance.
Source: http://www.latimes.com/news/nationworld/nation/wire/sns-ap-us-metro-workers-killed,0,808728.story

17. *January 25, WTKR 3 Norfolk* – (Virginia) **TSA director at Norfolk International Airport accused of not following screening procedures.** One of the TSA directors in charge of security screening at Norfolk International Airport has been accused of not following screening procedures. The matter has sparked an investigation involving the Transportation Security Administration. Security screening at the airport is not optional. Yet, a ranking security director at Norfolk International Airport has been accused of breaking the very protocol that his agency requires of all passengers. Sources tell NewsChannel 3 that when the Assistant Federal Security Director passed through initial security last week he was asked to submit to an additional screening. A secondary screening can be random or brought on by an alarm. He allegedly declined a second screening citing TSA protocol. Sources close to the investigation tell NewsChannel 3 that TSA agents typically do not "second screen" their own. TSA released this statement: "A full investigation into this matter is currently underway. Disciplinary action will be taken, if necessary." When asked if there was a breach in security, TSA said, "The individual in question was fully screened and there was no security breach." The incident did not rise to a level to involve airport police, however, a TSA source who witnessed the event tells NewsChannel 3 an employee not involved in the screening filed a complaint. The investigation will be a matter of how to interpret protocol regarding whether or not fellow TSAs are allowed to pass on second screenings.
Source: http://www.wtkr.com/news/wtkr-accused-tsa-airport,0,7401119.story

18. *January 25, KTRK 13 Houston* – (Texas) **TSA investigating traveler's gun claim.** The Transportation Security Administration is investigating whether an air traveler illegally carried a gun with him on a flight. The flight last month originated at Bush Intercontinental in Houston and traveled to Costa Rica. TSA officials say upon landing, the passenger went to the U.S. Embassy and admitted he had traveled with a gun. The TSA is still looking into whether the man had the gun checked in his baggage or if he carried it on board. Passengers can carry guns in checked baggage as long as they are unloaded and appropriately locked in a hard case.
Source: http://abclocal.go.com/ktrk/story?section=news/local&id=7238683

19. *January 25, Chicago Breaking News* – (Illinois) **Mini liquor bottle causes evacuation of plane at Midway.** The discovery of a miniature liquor bottle was a big enough concern to force a Southwest Airlines plane back to the gate at Midway Airport, where passengers were evacuated and the jetliner searched. The bottle had a clip attached and was apparently used by a flight attendant on the plane's previous flight to keep track of drink receipts, sources said. As Flight 2543 was leaving the gate around 1:15 p.m. Monday, bound for Detroit, an attendant noticed the bottle and took it to the pilot, who decided to return, the airline said. The Transportation Security Administration issued a brief statement saying, "the pilot returned the plane to the gate where all passengers and carry-on items were rescreened, with negative findings." The Boeing 737 was cleared for departure, the TSA said.
Source: http://www.chicagobreakingnews.com/2010/01/southwest-plane-evacuated-searched-at-midway-airport.html

20. *January 25, Associated Press* – (Florida) **Concourse temporarily closed at Miami International Airport after suspicious bag found.** A concourse at Miami International Airport was closed for several hours after authorities discovered a suspicious suitcase. The Transportation Security Administration says a Miami-Dade police dog alerted officers to a bag in Concourse J on Monday afternoon. The concourse, which handles mostly international flights, was evacuated, but the rest of the airport remained open. Authorities were interviewing the bag's owner. The suspicious bag was removed by a Miami-Dade bomb squad robot. It was not immediately clear if the bag was a legitimate threat. An airport spokesman says the concourse has since been reopened.
Source: http://www.latimes.com/news/nationworld/nation/wire/sns-ap-us-miami-concourse-closed,0,1964198.story

For more stories, see items **1**, **4**, and **45**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

21. *January 23, Marshall County Pilot News* – (Indiana) **Madras fire contained to ceiling, roof.** A fire that started in the Madras Packaging production area was blamed on a faulty electrical crossbar, according to Madras Packaging vice president and general manager. "It could have been worse," he said. "We're very thankful no one was hurt." He said once the fire started, it moved through the ceiling of the factory. "We evacuated," he said, adding that Madras em-ploys 20 production people; 80 in all at the plant that is a plastic bottle and container manufacturer for juice and dairy producers.

He said he expects production be back up and running within five days. The Argos fire department was assisted by Plymouth, Rochester and Culver. Around 30 firefighters helped fight the stubborn slow burn in the ceiling and roof.
Source: http://www.thepilotnews.com/content/view/147308/27/

[Return to top]

Water Sector

22. *January 26, Newport News Daily Press* – (Virginia) **Virginia scraps its annual water pollution monitoring program.** Tasteless, odorless and nearly as clear as water, polychlorinated biphenyls are among the most dangerous toxic chemicals in Virginia's waterways. Every year, state officials monitor the chemicals, known as PCBs, by testing fish from selected river basins, with fish advisories following. Facing a $5 million funding cut, the state Department of Environmental Quality (DEQ) last summer scrapped the $365,000 PCB monitoring program. It will now check for the chemicals on an as-needed basis. DEQ began routine monitoring for PCBs in 1998. It targets several river basins per year, taking samples from 50 to 100 locations. If possible, biologists collect a handful of top-level predators (e.g. largemouth bass), mid-level predators (e.g. bluegill), and bottom-feeders (e.g. catfish) at each location. Opponents of the funding cut are pushing the General Assembly to reauthorize the contract or to introduce new legislation to secure funding. A DEQ spokesman said the agency is not required to test for PCBs. Virginia law states that fish tissue and sediment be monitored at least once every three years "contingent upon the appropriation of adequate funding." There is also some debate whether such intense testing is necessary. Neighboring states, such as North Carolina and West Virginia, do not annually monitor PCBs. The reason: scientists know where the chemicals are, and tests are relatively expensive.
Source: http://www.dailypress.com/news/dp-local_pcbs_0123jan26,0,118343.story

23. *January 26, Austin American-Statesman* – (Texas) **Austin may spend $525,000 more to dismantle water plant.** The City of Austin, Texas, is poised to spend an additional $525,000 on dismantling the downtown Thomas C. Green Water Treatment Plant to pay for more inspections and other work officials say became necessary after the city found serious workplace safety violations at the site. On Thursday, the City Council will vote on whether the city should amend its contract with engineering firm URS Corp., which would be paid as much as $3.43 million to handle the engineering and oversight of the Green project. The Green plant was decommissioned a year ago and will be torn down to make way for a mix of shops, offices, condominiums and other projects. But work on Green has been stopped since December 4 , after inspectors found what the director of the city's Public Works Department characterized as "serious safety violations," including sending workers into tight spaces such as storage tanks and utility tunnels with inadequate safety precautions. The director expects work to resume in the coming weeks . He said the general contractor, Austin Filter Systems, has responded to the city's concerns — for instance by firing two subcontractors in response to the safety violations — but has not yet submitted a revised timeline for the

plant dismantling.
Source: http://www.statesman.com/news/local/austin-may-spend-525-000-more-to-dismantle-195550.html

24. *January 26, NaturalNews* – (National) **EWG study finds hundreds of pollutants in nation's drinking water.** The Environmental Working Group (EWG) has released a report indicting the nation's drinking water supplies are being highly contaminated with pollutants. An analysis of 20 million water quality tests performed between 2004 and 2009 revealed that many local and regional water supplies are tainted with up to 316 different toxic chemicals, many of which are unregulated by current federal standards. Of the over 300 pollutants found, the Environmental Protection Agency (EPA) has set safe maximum limits for only 114 of them, leaving the remaining 64 percent unrecognized as pollutants and unregulated by toxin laws. Nearly 10,000 American communities comprised of roughly 132 million people are receiving over 200 unregulated chemicals in their water supplies. Experts question the long-term safety of ingesting such tainted water, citing the fact that even existing federal laws about regulated chemicals suggest that tap water is unsafe for long-term ingestion. The senior vice president for research at EWG notes that federal guidelines have failed to keep up with the growing number of toxic contaminants being found in drinking water. Utility companies, she says, are doing their best to purify water and make it safe to drink, but federal laws must be amended to include new chemicals in order to protect water supplies from unnecessary contamination.
Source: http://www.naturalnews.com/028026_drinking_water_pollutants.html

[Return to top]

Public Health and Healthcare Sector

25. *January 26, Rapid City Journal* – (South Dakota) **Eagle Butte dialysis patients evacuated after power fails.** The power outages and water shortages plaguing most of north central South Dakota made refugees out of 35 kidney dialysis patients from the Cheyenne River Sioux Tribe and their caregivers, stranding them in Rapid City. Patients who receive dialysis three times a week at Eagle Butte on the reservation were evacuated Friday after snow and wind storms cut power to large sections of north central South Dakota. Most had little or no warning that they were leaving. Some arrived without their medicines, toiletries, money or clothing. Providing for the needs of patients and caregivers has been a challenge. It is uncertain when people can return home. Some patients were initially sent to Bismarck, Aberdeen or Pierre, but all were eventually routed to Rapid City. Those going to Pine Ridge were sent with sack lunches provided by the Rapid City Indian Hospital (Sioux San). The Travelodge allowed the group to use its kitchen to store and distribute food. The Golden Corral and the Millstone restaurants delivered warm meals on Saturday and Sunday evening. The CornerStone Rescue Mission provided some sack lunches over the weekend. By Monday, the American Red Cross, Salvation Army, National Relief Charities and Western South Dakota Community Action were working to provide clothing, food, personal hygiene items and other necessities for the displaced people. Indian Health

Services plans to move patients receiving treatment at Pine Ridge to the Prairie Winds Casino. One care giver said it would be at least three days after the power and water are restored before the dialysis center in Eagle Butte can accept patients.
Source: http://www.rapidcityjournal.com/news/article_ec833f00-0a38-11df-a62b-001cc4c002e0.html

26. *January 25, Associated Press* – (Maryland) **Chemical lab fire destroys gear in Hagerstown, MD.** The operator of a Hagerstown, Maryland, laboratory where an overnight fire destroyed thousands of dollars worth of equipment says safety policies and procedures prevented worse damage. The president of Tox Path Specialists LLC at Hagerstown Community College said Monday the fire may have stemmed from a malfunction in an incubator where tissue samples stained with an alcohol solution are routinely left to dry overnight. He says a vent on the device may have been partially blocked, causing combustion of the vapors that had accumulated under a hood. He estimated the damage at just over $2,000; the Maryland State Fire Marshal put it at $7,500.
Source: http://wjz.com/wireapnewsmd/Chemical.fire.destroys.2.1447150.html

27. *January 25, American Medical News* – (National) **Phishing schemes are becoming sneakier in targeting doctors.** A faculty physician at the University of California, San Francisco, Medical Center received an e-mail last fall appearing to be from the hospital's information technology staff. The e-mail requested the doctor's login information in order to perform routine security upgrades to the system. Because it seemed like an ordinary request, the physician sent the information. But that e-mail was from a scammer, and by responding, the physician had unwittingly exposed the personal information of more than 600 of his patients. This type of scam has become so common it has earned its own nickname: "spearphishing." One recent phishing case was carried out by scammers who posed as the Centers for Disease Control and Prevention and sent e-mails to patients and doctors claiming everyone had to register at an online H1N1 vaccine database. A link in the e-mail took unsuspecting recipients to a Web site that looked as if it was operated by the CDC. A warning issued later by the real CDC indicated hackers were likely sending malicious software downloads to victims' computers. Many times scams directed at physicians are facilitated by disgruntled employees who can identify parties that commonly reach the practice by e-mail, such as hospitals, contracted insurers, billing clearinghouses, and technology vendors, said the director of security intelligence at VeriSign iDefense. If a system is exposed to a virus, the scammers will likely gain access to patient lists and use those to target patients. Doctors should make it a habit to remind patients the practice will never ask for personal information via e-mail, experts say. Physicians should also make their employees aware of possible scams, especially those staff members who routinely communicate with insurers and financial institutions.
Source: http://www.ama-assn.org/amednews/2010/01/25/bil20125.htm

[Return to top]

Government Facilities Sector

28. *January 26, Associated Press* – (New Jersey; National) **Grenade launcher, weapons cache, military map found in NJ motel room after man's arrest.** Authorities in central New Jersey have seized a cache of weapons and ammunition including rifles, a grenade launcher, and a night vision scope from the motel room of a Virginia man. The Somerset County prosecutor says the suspect, a 43-year-old Navy veteran from Reston, Virginia, also had maps of a U.S. military facility and a town in another state. He was arrested in Branchburg, New Jersey early Monday by officers responding to a report of a suspicious person. The FBI says the suspect has no known terrorism links. The Somerset County prosecutor says the suspect was wearing a bulletproof vest and carrying a semiautomatic Bushmaster rifle under his jacket when he was arrested. The suspect was being held at the Somerset County Jail on charges including unlawful possession of weapons. The suspect had been staying at the Red Mill Inn in Branchburg.
Source: http://www.latimes.com/news/nationworld/nation/wire/sns-ap-us-nj-weapons-arrest,0,1633106.story

29. *January 26, Associated Press* – (Georgia) **Fort Benning protesters get maximum sentence.** Three people accused of trespassing on Fort Benning were convicted and given the maximum penalty of six months in prison. The protesters took part in annual demonstrations in November against the Western Hemisphere Institute for Security Cooperation, formerly known as the School of the Americas. The school trains Latin American soldiers, and opponents say it is linked to human rights violations in Latin America. The Columbus Ledger-Enquirer reports that the three protesters were sentenced Monday. A fourth protester did not appear. A warrant was issued for his arrest. Protesters are frequently arrested during the annual protest, but the organizer said Monday's sentences were harsher than usual.
Source:
http://www.armytimes.com/news/2010/01/ap_benning_protesters_sentenced_012610/

30. *January 25, KMPH 26 Fresno* – (California) **Hazmat situation at Fresno federal courthouse.** A hazmat situation has been reported at the Fresno Federal Courthouse. Fresno City Fire crews are on the scene, where they are investigating a suspicious package found at the building. The package contained a small amount of a white substance. No evacuations have been made as of noon. The courthouse is located at Tulare and P Streets in Downtown Fresno.
Source: http://www.kmph.com/Global/story.asp?S=11876974

31. *January 25, KFSN 30 Fresno* – (California) **High school evacuated after bomb threat.** The Central High School East Campus had to be evacuated Monday morning after a report of a bomb on campus. The threat was called in over the weekend, but it kept kids out of class for about 45 minutes on Monday morning. When school officials received the message, they searched the school and found a suspicious package. The Fresno Police Department's bomb squad was called in to check the package. The package was determined to be non-threatening. All students are safe and back in class. The Fresno Police Department is still investigating the source of the voice-mail

message.
Source: http://abclocal.go.com/kfsn/story?section=news/local&id=7236850

32. *January 22, Examiner* – (Tennessee) **200K worth of energy drink stolen from Navy base.** Two truck drivers have been charged with stealing government property after they allegedly snatched $200,000 worth of Red Bull energy drink from the commissary at Millington Naval Support Activity Mid-South in Millington, Tennessee. They are charged with theft of government property after their truck was stopped the week of January 11 and was found to be carrying 100 cases of the energy drink valued at $3,360, according to federal court documents released January 19. One of the men allegedly told authorities that he was responsible for stocking the shelves and displays with Red Bull at the commissary and that he and his assistant had been stealing the drink routinely since June 2007. It is believed that they had taken an estimated $200,000 worth of the drink during that time. Authorities said the pair were captured on videotape earlier this month, showing one moving pallets of the energy drink to a rear cargo door of the commissary and then helping the other load the drinks into a rental truck.
Source: http://www.examiner.com/x-31965-Military-Headlines-Examiner~y2010m1d22-200K-worth-of-energy-drink-stolen-from-Navy-base

[Return to top]

Emergency Services Sector

33. *January 25, San Diego North County Times* – (California) **Two people caught trying to deflate patrol car tires.** Sheriff's deputies want to make sure people know that tampering with emergency vehicles is no joke after a pair of pranksters was caught Saturday in Vista trying to deflate the tires of two patrol cars. Deputies were on a break eating at the In-N-Out Burger restaurant when an off-duty community service officer told them someone was tampering with their vehicles. The officer watched two people try to remove the tire stems at about 1:30 a.m. Two people, ages 27 and 29, were arrested for allegedly being drunk in public and face charges of conspiracy to commit a crime and tampering with a vehicle, according to a police sergeant. "They thought it was a joke," he said. "We consider this very serious. If deputies got called away from lunch to respond to an emergency, that could lead to someone getting hurt, because it would slow our response time."
Source: http://www.nctimes.com/news/local/vista/article_f71aab64-d79a-5cd9-b7be-7e9245772d27.html

34. *January 25, WSPA 7 Spartanburg* – (South Carolina) **Union police officer's stolen gun used in shooting.** Investigators say a handgun recently stolen from a police officer's personal vehicle was used in a drive-by shooting. According to an incident report from the Union County Sheriff's Office, a Union Public Safety Officer came to the sheriff's office on January 18th to report that his duty belt had been stolen from his truck. The duty belt contained a .40-caliber Glock handgun, 32 rounds of ammunition, pepper spray, handcuffs,and other official equipment. On the following day, deputies

were called to a shooting on Rogerstown Road in Jonesville. Reports state three teenagers had gone there to fight another teen. After fighting in the yard, the three teens got into a car and drove past the house, firing three shots as a woman and her son stood in the front yard. No one was injured. Three teens turned themselves later that day. Investigators say on January 21st, while in jail, one (age 18) gave a statement voluntary statement saying that he had fired the shots, and he had stolen the gun he used in the shooting from a red Chevrolet pickup truck parked at the officer's home. He said he and another teen were walking the neighborhood, looking for cars to break into, when they found the truck was unlocked and then found the officer's duty belt inside. The gun and the gun belt were recovered and all three teens were charged with assault and battery with intent to kill, assault with intent to kill, and various other charges. The Union Public safety chief says he cannot discuss whether or not the officer is being disciplined, citing "personnel matter", but he says it was clearly wrong of him to leave his weapon in his vehicle. He says he is drafting a policy for his department that will spell out how officers are supposed to secure their guns and ammunition when they are off-duty.
Source:
http://www2.wspa.com/spa/news/local/article/union_police_officers_stolen_gun_used_in_shooting/32359/

35. *January 25, WTSP 10 St. Petersburg* – (Florida) **Teen with bat smashes six sheriff's cars.** A teenager (age 17) smashed the windows and windshields of six sheriff's cars parked inside the sheriff's operations center parking lot Monday in Bradenton, Florida. He was charged with felony criminal mischief. Deputies said he damaged administrative and pool vehicles, smashing windows, windshields and two spotlights. A K-9 deputy arrived to see the vandalism in progress and took the suspect into custody, the sheriff's office said. All of the vehicles were towed away for repairs. The motive for the crime was not reported.
Source: http://www.wtsp.com/news/local/story.aspx?storyid=123606&catid=8

[Return to top]

Information Technology Sector

36. *January 26, The Register* – (International) **'Aurora' code circulated for years on English sites.** An error-checking algorithm found in software used to attack Google and other large companies circulated for years on English-speaking websites, casting doubt on claims it provided strong evidence that the malware was written by someone inside the People's Republic of China. The smoking gun said to tie Chinese-speaking programmers to the Hydraq trojan that penetrated Google's defenses was a cyclic redundancy check routine that used a table of only 16 constants. A security researcher said the algorithm "seems to be virtually unknown outside of China," a finding he used to conclude that the code behind the attacks dubbed Aurora "originated with someone who is comfortable reading simplified Chinese." "In my opinion, the use of this unique CRC implementation in Hydraq is evidence that someone from within the PRC authored the Aurora codebase," the researcher wrote. Two weeks ago, Google said it

was the victim of highly sophisticated attacks originating from China that targeted intellectual property and the Gmail accounts of human rights advocates. The company said similar attacks hit 20 other companies in the internet, finance, technology, media and chemical industries. Independent security researchers quickly raised the number of compromised companies to 34. But Google provided no evidence that China was even indirectly involved in the attacks targeting its source code. During a conference call last week with Wall Street analysts, Google's CEO said only that the world's most populous nation was "probably" behind the attacks.
Source: http://www.theregister.co.uk/2010/01/26/aurora_attack_origins/

37. *January 26, SC Magazine* – (International) **TechCrunch blog hit by hackers on the day before the Apple launch.** The TechCrunch website is back online after being hacked early on January 26. At approximately 6:20am GMT, the website was replaced with a message that stated: 'What a f***ing useless hack isn't it? Bleh'. A link was also given that connected to a site that contained links to adult material. The hack did not last long however. The senior technology consultant at Sophos reported at 9.15am GMT that the message on the TechCrunch site now reads 'earlier tonight techcrunch.com was compromised by a security exploit. We're working to identify the exploit and will bring the site back online shortly'. At 10.05am GMT it was back up-and-running again. An update by site engineer said: "As some people noticed, at approximately 10:30pm PST on on January 25 the main site in the TechCrunch Network – techcrunch.com – was hacked and redirected. The site was back up briefly at 11:30pm but shortly went down again. As of 2:00am, the site is back up and appears to be stable."
Source: http://www.scmagazineuk.com/techcrunch-blog-hit-by-hackers-on-the-day-before-the-apple-launch/article/162316/

38. *January 25, Computerworld* – (International) **Google patches 13 Chrome bugs, adds extensions to Windows.** Google on January 25 added support for extensions and bookmark synchronization to the production version of Chrome for Windows. The new release also patched 13 security vulnerabilities in the browser, six of which Google ranked as "high" in its threat scoring system. Although a beta of Chrome in December 2009 included support for both extensions and bookmark sync, this is the first time that the features have appeared in the "stable" build channel, a term Google uses in place of "final." Google also touted the growth of its extension gallery, which now has more than 1,500 add-ons, a five-fold increase over the 300 available at its debut in December 2009. Only Windows' stable edition supports extensions and sync; Linux users must use the beta channel build for the same features, while Mac owners have to drop all the way down into the least reliable version, dubbed the "developer" build by Google, to access extensions.
Source:
http://www.computerworld.com/s/article/9148278/Google_patches_13_Chrome_bugs_adds_extensions_to_Windows

39. *January 25, IDG News Service* – (International) **Researcher to reveal more Internet Explorer problems.** Microsoft's Internet Explorer (IE) could inadvertently allow a

hacker to read files on a person's computer, another problem for the company just days after a serious vulnerability received an emergency patch. The problem was actually discovered as long as two years ago but has persisted despite two attempts by Microsoft to fix it, said a security consultant with Core Security Technologies. He is scheduled to give a presentation at the Black Hat conference in Washington, D.C., on February 3. The issue could allow a hacker to read files on a person's computer but not install other code. Nonetheless, the problem represents a serious security issue, the consultant said. It affects all of Microsoft's operating systems from Windows NT through Windows 7 and every version of IE, including the latest one, IE8. The hack works when an attacker lures a victim into clicking on a malicious URL (Uniform Resource Locator). Then, by manipulating four or five features in Internet Explorer, the hacker forces the browser to process files that are not pure HTML on the PC, the consultant said.
Source:
http://www.computerworld.com/s/article/9148138/Researcher_to_reveal_more_Internet_Explorer_problems

40. *January 25, DarkReading* – (International) **Flaws in the 'Aurora' attacks.** The attackers who unleashed the recent wave of targeted attacks against Google, Adobe, and other companies made off with valuable intellectual property and source code and shocked the private sector into the reality of the potential threat of state-sponsored cyber-espionage — but they also made a few missteps along the way that may have prevented far worse damage. Security experts say while the attacks indeed were potent in their outcome, they were discovered relatively quickly by Google, and the malware used to attack Google, Adobe, and other as-yet unnamed companies was not especially sophisticated nor unique other than the fact that it was a zero-day exploit. The attacks — which Google says came out of China — had been underway for on average for nearly a month, and Google found them out in mid-December. Chinese officials on January 24 told the state-run Xinhua news agency that the government was not involved in the attacks. What impressed security researchers who've studied the code was the outcome of the attacks, not the malware. "The sophistication of the Aurora attacks is less about the malware and zero-day used, and more about the coordinated effort to target and pilfer from an estimated 33 companies in a short period of time," said the chief security architect for FireEye.
Source:
http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=222500010

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

41. *January 25, Orange County Register* – (California) **AT and T phone service down in parts of Laguna Woods.** An AT&T cable damaged by water from last week's storms has left customers in Laguna Woods, Lake Forest and Laguna Hills without service, a spokeswoman said. The company has crews working on the problem at El Toro Road and Muirlands Boulevard in Lake Forest, and phone service is expected to be restored by January 26, said a AT&T spokeswoman. The spokeswoman said she did not know how many customers were affected, but she said the cable serves up to 1,200 phone lines. Repair crews were working on January 25 to dry out the cable and replace a connector piece that was damaged by water, the spokeswoman said. Separately, flooding of an underground telephone vault near Moulton Parkway and Via Campo Verde in Laguna Woods damaged circuits serving Laguna Woods Village, according to an individual who handles public relations for PCM, the community's property management company.
Source: http://www.ocregister.com/news/service-230827-phone-laguna.html

42. *January 25, Sand Springs Leader* – (Oklahoma) **Phone service cut and restored to Case Center, surrounding area.** A construction accident on January 25 has cut phone service to the Case Community Center, as well as to surrounding businesses and residences, a city spokesman said. Phones were down at the Case Center until 4 p.m., the spokesman added. A contractor doing work for the Wekiwa Road widening project severed a major telephone line there.
Source: http://www.sandspringsleader.com/articles/2010/01/25/news/doc4b5dd96c175a5396736907.txt

[Return to top]

Commercial Facilities Sector

43. *January 25, Norwich Bulletin* – (Connecticut) **Crystal Mall evacuated for unknown substance.** State officials are trying to identify the substance that led to the evacuation of Crystal Mall in Waterford, Connecticut on Monday afternoon. Assistant chief of the Cohanzie fire company said they were called out at 3:17 p.m. to a report of an unknown hazardous material after a person in the mall detected the odor of gasoline. He said an entry crew located a substance that it could not identify, and backed out before calling hazardous materials crews from the Groton Navy Base and the Connecticut Department of Environmental Protection. The substance was taken to a DEP facility for analysis. No one was hurt.
Source: http://www.norwichbulletin.com/newsnow/x1090820202/Crystal-Mall-evacuated-for-unknown-substance

44. *January 25, Associated Press* – (California) **Nebraskan to plead guilty to cyber attack on Church of Scientology.** Federal prosecutors in California say a Nebraska man will plead guilty to participating in a cyber attack on Church of Scientology Web

sites in January 2008. A spokesman for the U.S. attorney's office in Los Angeles, says the man agreed to plead guilty Monday to the misdemeanor charge of unauthorized access of a protected computer. He faces a year in federal prison. Court records say the man attacked Scientology Web sites as part of anonymous, an underground group that protests the Church of Scientology, accusing it of Internet censorship. Prosecutors say hackers conducted a "denial of service" attack, in which computers flood a target Web site with malicious Internet traffic, making it unavailable to legitimate users. Prosecutors say the man, of Grand Island, Nebraska is expected to enter his plea next week in Los Angeles, where the Church of Scientology is based.
Source:
http://www.argusleader.com/article/20100125/UPDATES/100126001/1001/NEWS

45. *January 25, Houston Chronicle* – (Texas) **Plane lands at Hermann Park Golf Course.** Golfers at Hermann Park may have some trouble navigating the course Tuesday morning because of an airplane sitting on the fairway. The pilot was not planning to provide local golfers a new type of hazard Monday evening when he made a bumpy but safe landing near the 11th hole. "The plane ran out of fuel," he said. "I thought I had another hour and a half on board but I didn't." He was flying the Cessna 170 single-engine private plane to Robert J. Wells Jr. Airport in Columbus when the engine started sputtering about 6 p.m. He notified local air traffic control and began to head toward Hobby Airport. A witness at the Houston Zoo near the golf course spotted the airplane making a series of tight turns. "Then it was diving for the golf course. It scared the hell out of us," he said. "I thought somebody was going to get killed." He was amazed that nobody was hurt in the landing. The pilot said his first concern was for the safety of the public. As the plane dropped toward the Hermann Park course, he spotted two fairways that looked like possible landing spots. "There was only one guy on this one, so I went over the top of him and landed," he said. He said the man dashed to safety. Houston police said officials with the Federal Aviation Administration are expected to arrive Tuesday to conduct an investigation into the forced landing.
Source:
http://www.chron.com/disp/story.mpl/metropolitan/6834950.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+houstonchronicle/topheadlines+(chron.com+-+Top+Stories)

For another story, see item **28**

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

46. *January 26, Winston-Salem Journal Reporter* – (North Carolina) **Surge of heavy rain causes mudslides.** Workers spent yesterday clearing debris from roads after Sunday's heavy rain caused mudslides and flooding in several parts of Northwest North Carolina. Three to five inches of rain fell Sunday night, leading to a mudslide early yesterday on Tobaccoville Road, about 1.5 miles west of Tobaccoville. A 14-foot high bank that included about 10 small trees and 200 tons of earth slid down and covered the westbound lane, said a division maintenance engineer for the North Carolina Department of Transportation. There were no injuries or damage to any homes or businesses. The road was still closed last night. There were also several mudslides in the mountains and foothills. At Salem Lake, water poured over the dam and into Salem Creek, flooding the greenway. Winston-Salem officials closed all of the greenways because of flooding. Tanglewood Park was partially submerged in water from the Yadkin River. Forecasters with the National Weather Service are expecting clear skies in Winston-Salem through Thursday afternoon. There will be a chance of rain on Thursday night, which could change to snow or freezing rain on Friday.
Source: http://www2.journalnow.com/content/2010/jan/26/surge-of-heavy-rain-causes-mudslides/

47. *January 26, Monroe News-Star* – (Louisiana) **Area levee damaged.** Joy riders carved deep ruts in the Tensas Basin levee on Ouachita City Road near Sterlington, Louisiana, last week, leaving the levee scarred and vulnerable as the Ouachita River remains above flood stage. The Tensas Basin Levee District executive director said, "We don't like to see it at any time, but especially not during high water." The Ouachita River has been above its 40-foot flood stage in Monroe for most of the past three months and remained at 41.2 feet on Monday. A two-mile stretch of the levee on Ouachita City Road is periodically striped by what looked like four-wheel drive truck tires. The high water levels have sofented the ground and made the levees more vulnerable to such abuse. The levees are off-limits to vehicle traffic and the Levee District Police issue citations to people driving on them. But someone who inflicts damage to the levee like that on Ouachita City Road is subject to a felony charge, which carries a prison sentence and fine.
Source: http://www.thenewsstar.com/article/20100126/NEWS01/1260315

48. *January 25, Associated Press* – (Washington) **Flood season may have passed for Green River Valley residents.** Forecasters say the Green River Valley may have dodged a significant flood and a potential disaster at the Howard Hanson Dam. King County declared a state of emergency, the brand-new elections office was closed and moved, and people were urged to buy flood insurance and sandbag their homes. Those were all necessary steps at the time, considering the threat created by the crumbling dam, but the flooding has not materialized, and the danger might have passed. "We should be cautiously optimistic that we may get through this season, but we're not there yet quite. We always have to be cautious. Mother Nature could throw us a curve ball pretty quick," said a meteorologist with the U.S. Army Corps of Engineers. He said the bulk of flooding season is behind us and the weather models show a drier pattern over the next couple of weeks. The experts say it is not time to start putting away sandbags or preparing for a flood, but it looks like people living and working along the Green

River can relax a bit for this year.
Source: http://www.mynorthwest.com/?nid=11&sid=275267

[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 Web site: 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