Homeland Security

Daily Open Source Infrastructure Report for 5 March 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- According to the Associated Press, Singapore's Navy issued a warning Wednesday that a terrorist group is planning attacks on oil tankers in the Malacca Straits, one of the world's busiest shipping lanes. (See item **1**)
- The U.S. Department of Justice announced that a suspect, who emigrated from Russia and set up numerous shell corporations in Oregon on behalf of Russian clients, was arrested Wednesday on charges of operating an unlicensed money transmitting business. The shell corporations allegedly were used to move more than $172 million into the United States and out to more than 50 countries. (See item **14**)

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. *March 4, Associated Press* – (International) **Singapore warns of terror threat in Malacca Strait.** Singapore's Navy warned that a terrorist group is planning attacks on oil tankers in the Malacca Straits, one of the world's busiest shipping lanes. Terrorists may also be targeting other vessels in the shipping lane off Malaysia's east coast,

according to an advisory issued on March 3 by the Navy's Information Fusion Center seen by the Associated Press. "The terrorists' intent is probably to achieve widespread publicity and showcase that it remains a viable group," the Navy advisory said. "However, this information does not preclude possible attacks on other large vessels with dangerous cargo." The Navy did not say which terrorist group is planning the attacks. Spokesmen at the Defense Ministry and the Information Fusion Center were not immediately available for comment. The Malacca Strait is the favorite route of oil shippers between the Persian Gulf and Asian Pacific markets. The strait, just 1.7 miles at its narrowest point, was the second-busiest shipping lane of crude in 2006, with 15 million barrels a day passing through, according to the U.S. Energy Information Agency. Singapore lies at the southern tip of the Malay peninsula and is home to the world's busiest port. The Navy said in previous successful terrorist attacks on tankers, small fishing boats or speedboats were used, and these kinds of boats could be used to attack ships in the Malacca Strait. The Navy, which said it is coordinating with regional partners regarding the threat, recommended ships add lookouts and lighting, avoid fishing areas, and maintain a good speed.
Source: http://www.forbes.com/feeds/ap/2010/03/04/general-as-singapore-terror-threat_7406113.html?boxes=financechannelAP

2. *March 3, U.S. Environmental Protection Agency* – (Connecticut) **Settlement resolves chlorine spills by Connecticut power plant.** The owner and operator of a coal-fired power plant in Montville, Connecticut, AES Thames, LLC, will pay a penalty of $140,000 to resolve alleged violations of the federal Clean Water Act and other environmental laws, arising from releases of chlorine from the plant to the Thames River in 2006. The Consent Decree also resolves alleged violations of steam production limits contained in AES Thames' Clean Air Act permit. AES Thames will pay the cash penalty of $140,000 and take measures to prevent repeat violations. In both January and March 2006, AES Thames had accidental spills of sodium hypochlorite (chlorine) into the Thames River. On both occasions, AES Thames also failed to notify emergency response agencies in a timely manner, in violation of the permit and other environmental statutes. AES Thames has revised and updated its Spill Prevention Control and Countermeasure Plan, its Stormwater Pollution Prevention Plan, its Chemical Handling and Spill Response Protocol, and its Emergency Action Plan safety protocol, to reflect and emphasize the correct regulatory requirements for reporting spills. In addition, AES Thames will conduct a Chemical Handling and Spill Response training annually for all employees. The training will emphasize the potential impacts of chemical spills on the facility's wastewater treatment system and the environment.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/eff78d72159b0b3a852576db006c3616?OpenDocument

3. *March 3, Reuters* – (Illinois) **One Peoples Gas worker killed in Chicago mishap.** One Peoples Gas company worker was killed and another injured on Wednesday in a mishap involving a pipe they were pressure-testing, Chicago authorities said. The workers were pressure-testing a 20-inch main pipeline with compressed air inside a reinforced hole near the Willis Tower in downtown Chicago

when the incident occurred, a Peoples Gas spokeswoman said. It was not immediately clear what happened, but no gas was involved and service was not interrupted, the spokeswoman said. A passerby told local radio he heard a "boom and then a whoosh" followed by a cloud of dust emerging from the hole. Another passerby climbed in to help before firefighters arrived to remove the workers. Peoples Gas, a regulated natural gas utility serving approximately 840,000 customers in Chicago, is a unit of Integrys Energy Group.
Source: http://www.reuters.com/article/idUSN03965902010030 3?type=marketsNews

4. *March 3, Port Huron Times Herald* – (Michigan) **No injuries in power plant fire.** The St. Clair Fire Department is investigating a fire that began March 3 inside the wall of a structure at the DTE Energy Belle River Power Plant and spread to the roof. St. Clair, Marine City, and Marysville fire departments responded to the fire at about 8:50 p.m., the St. Clair fire chief said. Crews cleared the scene at about 10:15 p.m. He said the fire was small, it did not interfere with the plant's operations, and there were no injuries.
Source: http://www.thetimesherald.com/apps/pbcs.dll/article?AID=2010100303019

5. *March 2, Environmental Protection* – (Oklahoma) **Coles Evergreen Marina pays fine, corrects SPCC violations.** The U.S. Environmental Protection Agency fined Coles Evergreen Marina of Stigler, Oklahoma $1,450 for violating federal Spill Prevention Control and Countermeasure (SPCC) regulations outlined under the Clean Water Act. A federal inspection of the Marina's bulk storage facility located at 113 E BK 800 Road in Haskell County, Oklahoma revealed the facility did not have an SPCC plan, and inspections and tests required by federal regulations were not in accordance with written procedures developed for the facility. Personnel working at the site had no training on the operation and maintenance of equipment to prevent discharges, discharge procedure protocols, and applicable pollution control laws, rules, and regulations. The inspection also found spill prevention briefings were not scheduled and conducted periodically, the facility was not fully fenced and entrance gates were not locked and/or guarded when site is unattended, and facility lighting was not adequate to facilitate the discovery of spills during hours of darkness and to deter vandalism. As part of an Expedited Settlement Agreement with EPA, the facility has provided certification that all identified deficiencies have been corrected.
Source: http://eponline.com/articles/2010/03/02/coles-evergreen-marina-pays-fine-corrects-spcc-violations.aspx

For more stories, see items **6** and **26**

[Return to top]

Chemical Industry Sector

6. *March 4, Homeland Security Today* – (National) **DHS supports IST for chemical facility security.** The U.S. Presidential Administration supports consideration of inherently safer technology (IST) for chemical facility security standards and the extension of those standards to water and wastewater facilities, the top infrastructure

protection official at the Department of Homeland Security (DHS) testified on March 3. The undersecretary for National Protection and Programs addressed the need to reauthorize the Chemical Facility Anti-Terrorism Standards (CFATS) administered by DHS and due to expire at the end of this fiscal year. He called upon the Senate Homeland Security and Governmental Affairs Committee for a permanent of authorization to the program, even if no changes were made to it, as it has worked well to strengthen chemical facility security. The Administration would submit suggested legislation on how to extend CFATS to include provisions on IST and water and wastewater facilities within several months, he predicted. DHS supports providing its regulators with the ability to require high-risk facilities to adopt IST if it becomes the best or only way to ensure security at a chemical facility, he said. IST methods seek to replace chemical engineering processes at plants with chemicals that might be less toxic to people or the environment and thus make a facility less attractive as a terrorist target. But the Administration would not blindly endorse IST, he cautioned. DHS would consider the economic impact, the timeframe, and any conflicts with public health or environmental requirements in doing so. In addition, experts have no common understanding of what IST actually requires, a U.S. senator argued. The undersecretary responded that DHS would work with industry to establish a consensus for the purposes of the law.
Source: http://www.hstoday.us/content/view/12388/128/

For another story, see item **31**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

7. *March 4, Rutland Herald* – (Vermont) **Leak a sign of bigger issues, NRC told.** The radioactive leak of tritium at the Vermont Yankee nuclear plant is just the tip of the iceberg of deferred maintenance, representatives for the New England Coalition said Wednesday during a meeting with the federal Nuclear Regulatory Commission (NRC). The watchdog group filed a petition with the NRC against Entergy Nuclear, the owner of Vermont Yankee, about a month ago, asking that the reactor be shut down until the source of the tritium leak was identified and shut off. While that immediate request was denied, the coalition is pushing for enforcement against Entergy Nuclear, saying the tritium leak is just an indication of a larger problem. The senior technical adviser for the coalition said the tritium leak was a strong indication "Entergy is again deferring maintenance." "The tritium leak is indicative of deeper issues at the Vermont Yankee plant," the technical advisor told NRC staff during a teleconference. In addition, he said, Entergy is not taking cues from other nuclear reactors with similar problems and doing preventive work.
Source: http://www.rutlandherald.com/article/20100304/NEWS02/3040348

8. *March 3, Greeneville Sun* – (Tennessee) **NRC reports on actions after incident at plant.** About 100 Erwin residents and Nuclear Fuel Services (NFS) employees gathered in the auditorium at Unicoi County High School on Tuesday evening to

observe an inspection team "exit meeting" hosted by the U.S. Nuclear Regulatory Commission (NRC). The meeting was held to discuss the results of an NRC "augmented inspection" of an October 13, 2009, incident at the plant in which NFS attempted to implement a new procedure for processing so-called "fines," or small particles of scrap radioactive aluminum, to remove uranium with nitric acid. A slide shown by the NRC during the meeting said NFS chose to process the small aluminum particles through a "bowl cleaning station" that normally was used to remove uranium caked inside centrifuge bowls by circulating nitric acid through the bowls. "This process produces nitrogen compound off-gasses (NOx) as a by-product of the nitric acid dissolution process," the slide said. An initial NFS laboratory analysis had determined that the fine particles of aluminum should not be processed in caustic solutions, another NRC slide said.
Source: http://www.greenevillesun.com/story/308384

For another story, see item **32**

[Return to top]

Critical Manufacturing Sector

9. *March 3, Consumer Affairs* – (International) **Nissan recalls more than 500,000 vehicles.** On the heels of Toyota's long-running woes and GM's steering-related recall this week, Nissan has announced the recalling of 539,864 trucks, sport-utility vehicles and mini vans in North America and some Asian and European markets. Nissan says the affected models may have problems with brake pedal pins and fuel gauges. The company says it discovered a production error in the brake pedal pin, which could cause the pedal to disengage. It said it had three reports of that happening, but no reports of injuries. The fuel gauge problem could cause the affected vehicles to incorrectly indicate the amount of fuel remaining in the tank. Models affected by the pedal pin recall are the Infiniti QX56 SUV, Titan pickup truck, Armada SUV and Quest minivan. The Frontier pickup truck, Pathfinder and Xterra SUV may have the fuel gauge problem.
Source: http://www.consumeraffairs.com/news04/2010/03/nissan_recall.html

10. *March 3, Reuters* – (National) **US investigates complaints about Toyota recall fix.** U.S. regulators on Wednesday reviewed 10 complaints that fixes made to recalled Toyota Motor Corp vehicles did not resolve unintended acceleration. The National Highway Traffic Safety Administration said it is reviewing reports that have been received since mid-February and are interviewing vehicle owners. The regulator said the allegations were unconfirmed. The NHTSA administrator, said in a statement that the agency wants to "get to the bottom" of the matter and ensure that Toyota is doing "everything possible" to address the situation. "If Toyota owners are still experiencing sudden acceleration incidents after taking their cars to the dealership, we want to know about it," the administrator said. Toyota said it would move quickly to investigate the new complaints. Toyota's U.S. sales chief told Congress last week that he does not believe current recalls will address all cases of unintended acceleration. NHTSA is

again reviewing whether there are glitches with Lexus and Toyota electronic throttles. Toyota, which has hired an independent consulting firm to examine the issue, said as late as Tuesday that exhaustive testing has found no problems with that system. Toyota said this week it had fixed more than 1 million of the more than 6 million cars and trucks subject to recalls in October 2009 and January. Recalls covered loose floor mats that can jam the accelerator and gas pedals that do not spring back as designed. Source: http://www.reuters.com/article/idUSN0312107720100304

[Return to top]

Defense Industrial Base Sector

11. *March 4, Space Mart* – (National) **USAF eyes mini-thrusters for use in satellite propulsion.** Mini- thrusters or miniature, electric propulsion systems are being developed, which could make it easier for the Air Force's small satellites, including the latest CubeSats, to perform space maneuvers and undertake formidable tasks like searching for planets beyond our solar system. Researchers at Massachusetts Institute of Technology are considering the advantages of electric propulsion over more traditional chemical rocketry. As a result, they have discovered "ionic liquid ion sources" which are the core elements of the mini-thruster. In addition to the benefits anticipated for small satellites, the technology may have applicability in completely different areas. The team is interested in the properties that allow advances in travel between different orbits in space and the ability for spacecraft to self-destruct upon controlled re-entry, therefore preventing the creation of additional space debris. Source: http://www.spacemart.com/reports/USAF_Eyes_Mini_Thrusters_For_Use_In_Satellite_Propulsion_999.html

12. *March 2, U.S. Air Force* – (National) **Air Force officials work on trimmed-down instrument landing system.** Officials from the 853rd Electronic Systems Group here are working to improve the transportability and deployability of instrument landing systems with an upcoming request for proposal for a deployable instrument landing system, or D-ILS. An instrument landing system is a precision-approach system that consists of hardware, including antennas and electronics, and a software application. "Having a mobile ILS system in the Air Force inventory will provide warfighters in theater with three major capabilities: the ability to convert a bare base into an operating airfield, the ability to augment an existing airfield or the ability to temporarily restore ILS capabilities at damaged airfields during humanitarian operations," said the 853rd ELSG commander. "The current fixed-based ILS systems are time-tested solutions that everyone in the aviation community has confidence in, since all major airports have been using this technology for more than 50 years," said the program manager for deployable air traffic control and landing systems. "However, fixed-base ILS systems are fairly large structures that require installation of concrete and utilize large containers of electronics and cabling. We are working to scale that system down and make it as lean as possible so a small number of folks can install, configure and

maintain the system in a deployed environment."
Source: http://www.af.mil/news/story.asp?id=123192862

[Return to top]

Banking and Finance Sector

13. *March 4, Washington Post* – (National) **Fed proposes limits on credit card penalty fees.** The Federal Reserve proposed restrictions Wednesday on penalty fees that credit card issuers can charge consumers, including limiting the amount of late fees. One of the most significant changes would prohibit card companies from issuing penalty charges larger than the amount of the violation, a common consumer complaint. For example, a person who is late on a $20 minimum payment could not be hit with a $39 late fee. In addition, if a card's spending limit is exceeded by buying a $2 cup of coffee, the penalty fee cannot exceed $2. The proposed regulations represent the Fed's latest efforts to comply with the sweeping credit card reform legislation passed by Congress last spring. The final phase of the legislation, slated to take effect in August, requires that any penalty fees be "reasonable and proportional" — and lawmakers left it to the Fed to determine exactly what that meant. The proposal also bans inactivity fees that some card companies have charged if consumers do not make new purchases and prohibits multiple penalty fees for a single transgression. Card issuers must notify consumers of the reason for any interest rate increases and are required to take a second look at any accounts that have had rate increases since January 1.
Source: http://www.washingtonpost.com/wp-dyn/content/story/2010/03/03/ST2010030303843.html

14. *March 3, U.S. Department of Justice* – (National) **Oregon man charged with operating illegal money transmitting business that moved more than $172 million through shell corporations in the United States.** A suspect, who emigrated from Russia and set up numerous shell corporations in Oregon on behalf of Russian clients, was arrested on March 3 on charges of operating an unlicensed money transmitting business, announced the assistant attorney generalof the Criminal Division and the U.S. attorney for the District of Oregon. The shell corporations allegedly were used to move more than $172 million into the United States and out to more than 50 countries. The suspect, a naturalized U.S. citizen living in Tigard, Oregon, was indicted by a federal grand jury on one count of operating an unlicensed money transmitting business after more than 4,200 wire transactions had been made. The indictment alleges that the suspect emigrated from Russia to the United States in 1998. In order to move money in and out of the United States, the suspect allegedly created various shell corporations under Oregon law, and then opened bank accounts, including accounts at Wells Fargo, Key Bank, Bank of America and Bank of the West, which he used to deposit money he received from his Russian clients. The suspect allegedly would then wire the money out of the accounts based on wire instructions he received from his clients.
Source: http://www.prnewswire.com/news-releases/oregon-man-charged-with-operating-illegal-money-transmitting-business-that-moved-more-than-172-million-through-shell-corporations-in-the-united-states-86282817.html

15. *March 3, Miami Herald* – (Florida) **SEC accuses Miami couple of running $135M Ponzi scheme.** On March 3, the Securities and Exchange Commission alleged in a civil complaint that a couple had defrauded hundreds of people, mostly elderly Cuban-Americans, as part of a long-running Ponzi scheme. In all, the SEC alleges, the couple duped investors to the tune of $135 million between 2002 and 2009. The federal agency also alleged that the couple used $20 million from investors to pay themselves exorbitant salaries, to invest in other projects and to divert some $1 million to their children and grandchildren in the form of alleged "consulting fees." SEC officials said the couple were not registered with the federal government to make securities offerings to investors. According to a statement, the SEC says that the Miami couple, who founded Royal West Properties Inc. in 1982, sold promissory notes to investors after acquiring various properties and later financing their sale. It further alleges that Royal West continued to offer credit schemes and real estate investments, particularly to Cuban and Latin American investors, even after showing operating losses as early as 2002.
    Source: http://www.miamiherald.com/2010/03/03/1510055/sec-accuses-miami-couple-of-running.html

16. *March 3, eSecurity Planet* – (International) **Database security lacking at financial services firms.** Sloppy operating practices across the financial services sector leave firms vulnerable to breaches that could expose sensitive data or put customers' and employees' privacy at risk, according to a new study from the Ponemon Institute. The study, commissioned by enterprise software and consulting firm Compuware, identified several key areas where financial services companies could take a hit from loose data policies, including damage to the corporate brand and the erosion of consumer trust. "One of the most important things a company can do to assure their future success is to plug the holes in their security policies that were demonstrated in this study," the head of the Ponemon Institute, said in a statement. "While there is a great deal of progress being made, there is still a long way to go." For instance, the survey of top security officials at 80 large financial firms found that 83 percent use real data, such as credit card or account numbers, when developing and testing applications. Ponemon concluded that a majority of the firms surveyed don't take sufficient steps to safeguard that information. The latest warning about information security comes amid a growing wave of data breaches that have targeted universities, insurance firms and others.
    Source: http://www.esecurityplanet.com/trends/article.php/3868381/Database-Security-Lacking-at-Financial-Services-Firms.htm

For another story, see item **49**

[Return to top]

Transportation Sector

17. *March 4, Asian News International* – (International) **Two Pak women barred from boarding plane for refusing UK airport body scan.** Two Pakistani women were barred from boarding a flight to Islamabad after they refused to undergo a full-body

scan at Manchester Airport, citing religious and medical reasons. According to reports, the women were warned that they would not be permitted to board their Pakistan International Airlines flight if they refused to undergo the scan. But the duo decided to forfeit their tickets rather than submit to the scan. The action was taken despite a British Transportation Security Administration assurance that going through scanners is optional. The two women are the first passengers to refuse scanning by machines. Scanning has provoked controversy among British human rights groups. "Two female passengers who were booked to fly out of Terminal Two refused to be scanned for medical and religious reasons. In accordance with the government directive on scanners, they were not permitted to fly," The Times quoted a Manchester Airport spokeswoman, as saying. "Body scanning is a big change for customers who are selected under the new rules and we are aware that privacy concerns are on our customers' minds, which is why we have put strict procedures to reassure them that their privacy will be protected," she added.
Source: http://www.dailyindia.com/show/362694.php

18. *March 4, Sarasota Herald-Tribune* – (Florida) **Emergency repairs to shut Venice runway.** A runway at the Venice Municipal Airport will be closed next week for emergency repairs that the city was supposed to have completed in January. The repairs were prompted by a Florida Department of Transportation letter found on the former Venice Airport Director's desk shortly after he was fired two weeks ago. A Venice spokeswoman said she "would not speculate" why the director did not inform the city manager of the December 2 letter, which detailed deficiencies from a state inspection two months earlier. The DOT cited "potholes and large cracks" in a 543-foot section of runway 4-22 that "may interfere with the directional control of landing aircraft." The area to be repaired includes the full width and about 10 percent of the runway length. The agency also demanded that markings on the runway be repainted.
Source: http://www.heraldtribune.com/article/20100304/ARTICLE/3041060/-1/NEWSSITEMAP?tc=ar

19. *March 4, Springfield News-Sun* – (Ohio) **Damaged bridge will close a lane of U.S. 68 at U.S. 40.** A spokeswoman from the Ohio Department of Transportation said a consultant will visit the bridge on U.S. 68 South at the U.S. 40 overpass. The consultant will do an analysis of the damage, and determine what repairs need to be made, she said. It is unclear how long the repairs will take, she said. In the meantime, ODOT has closed the left passing lane and left shoulder of the road. One lane of traffic will remain open for southbound drivers. Arrow boards and signs will be in place to alert drivers about the lane closures. Drivers are being asked to remain alert, reduce speed and watch for stopped traffic while passing through the work zone. The public should also expect short lane closures on a regular basis for follow-up inspections after the repairs, according to information from ODOT. A semitruck trailer pulling a forklift east on U.S. 40 had its boom up in the air, which struck a steel beam of the overpass on U.S. 40 and Ohio 4, according to a Ohio State Highway Patrol trooper.
Source: http://www.springfieldnewssun.com/news/springfield-news/damaged-bridge-will-close-a-lane-of-u-s-68-at-u-s-40--578034.html

20. *March 4, Reuters* – (Illinois) **Chicago's O'Hare lax on security, ex-chief charges.** In a lawsuit filed in Cook County Court, the former chief of security at O'Hare airport said the Chicago City Aviation commissioner and her staff "continually ignored, dismissed and shunned [him] in his efforts to make O'Hare Airport a safer facility." The chief had spoken out repeatedly about "potentially catastrophic terrorist opportunities at O'Hare Airport," said the lawsuit that named two airport officials and the city of Chicago as defendants. The suit said airport executives lacked experience in policing and anti-terrorism strategies, and appeared to be solely concerned with the $15 billion modernization and expansion plan under way at O'Hare. Among the security threats cited in the suit were a shortage of patrol officers and allowing some 10,000 private vehicles owned by airline workers to be parked inside the security perimeter at O'Hare. The suit said it would not detail other security gaps for fear that the information might fall into the wrong hands. The former chief said O'Hare is "the least secure airport in the country" in an interview with the Chicago Sun-Times newspaper. The former chief said he was improperly fired last year based on what he said were false allegations that he had assaulted an airport executive.
Source: http://www.reuters.com/article/idUSN0411408220100304?type=marketsNews

21. *March 4, CNN* – (International) **Investigators on way after waves kill cruise passengers.** Investigators were en route Thursday, and dead and injured were being evacuated, a day after 26-foot waves crashed into a cruise ship and killed two people off northeast Spain, officials said. The Greece-based Louis Cruise Lines ship was in the Mediterranean north of Barcelona, Spain, when it was hit by three "abnormal" waves, each about 26 feet high, said a cruise line spokesman. The waves smashed five windows on deck five in public areas — on the forward part, or bow, of the 14-deck ship. Two passengers were killed. The first wave pushed down the ship's bow, and the second wave soon after struck the front of deck five. Crew members evacuated the injured to the ship's hospital. Several doctors and nurses traveling aboard as passengers also helped. Fourteen were treated aboard the ship for light injuries, but were hospitalized as a precaution when the ship returned to Barcelona on Wednesday night. The incident occurred 24 miles off Cabo de San Sebastian, near the Spanish town of Palafrugell. The ship had 1,350 passengers and 580 crew members, the Greek ministry said. The passengers were from 27 nations. They included Americans, French, Germans, and Italians.
Source:
http://www.cnn.com/2010/WORLD/europe/03/04/spain.cruise.ship.wave/index.html?hpt=Sbin

For more stories, see items **1** and **43**

[Return to top]

Postal and Shipping Sector

22. *March 3, Atlanta Journal Constition* – (Georgia) **Powdery substance causes scare in Gilmer County, again.** For the second straight day, Gilmer County dealt with a scare

over an envelope containing suspicious white powder Wednesday. Both incidents appear to be hoaxes. The envelope found Wednesday morning at Gilmer County High School in Ellijay prompted officials to close school for the day while authorities investigate. The FBI, GBI, and a hazardous materials team from Cherokee County were still at the scene in the afternoon. On Tuesday, a similar envelope was found at the Gilmer County courthouse. "They investigated and found that was just a hoax, not a volatile substance," said a spokesman for Gilmer County schools. "People processing the mail this morning at Gilmer County High School came across another envelope with a powdery substance. Same M.O., same handwriting. Looks very similar." By Wednesday evening, the spokesman said the substance found at the school was determined to be nothing dangerous or hazardous. It is being sent to a lab for further analysis, he said. School was closed due to snow Tuesday and scheduled to start two hours late Wednesday. As students and staff arrived, they were told to go home.
Source: http://www.ajc.com/news/powdery-substance-causes-scare-344265.html

23. *March 3, Salt Lake Tribune* – (Utah) **Prisoner charged with sending anthrax threats through mail.** A Utah prison inmate who allegedly sent an anthrax threat to at least one government office in Salt Lake City last December now faces federal charges. The inmate was charged Wednesday with two counts of mailing threatening communications concerning an anthrax hoax, the indictment states. The Utah Department of Corrections, in December 2009, contacted several government agencies after the inmate told investigators he sent a letter containing an anthrax threat. The inmate later admitted the letter did not contain anthrax. Officials, at the time, informed several government agencies, including the Utah Attorney General's Office, to alert them of the scare. The offices were only contacted as a precaution.
Source: http://www.sltrib.com/news/ci_14508039

[Return to top]

Agriculture and Food Sector

24. *March 4, Reuters* – (North Carolina) **ConAgra to close damaged Slim Jim plant.** Packaged foods maker ConAgra Foods Inc. plans to shut a North Carolina Slim Jim meat snacks plant where three people were killed in a June 2009 explosion. The closing of the plant in Garner, North Carolina, will result in about 500 jobs being cut, though 200 jobs will be added to a plant in Troy, Ohio, where production will be moved, the company said on Thursday. The North Carolina plant operated at limited capacity after the June explosion that caused a roof to collapse, killing three workers and injuring more than 40 other people. The closing is expected to result in charges of $52 million to $72 million, while the company will also spend $60 million to $70 million at the Troy plant, ConAgra said.
Source: http://www.reuters.com/article/idUSN0423410220100304?type=marketsNews

25. *March 4, Associated Press* – (Michigan) **Explosion halts factory's potato chip production.** Workers at the Better Made Snack Foods factory in Detroit have been sent home after an explosion in the oil heating process for potato chips shook parts of the

building. The company chief executive says it appears pressure built up in a heat exchanger in one of the east side factory's four fryers about 9:30 a.m. Thursday. The blast damaged some ceiling tiles and broke a few windows. He says no one was injured and potato chip-making operations likely will be stopped until Monday. The manufacturing operation typically is shut down on Fridays. He says the work stoppage likely will not affect chip sales. The company has about 90,000 cases in its warehouse.
Source: http://www.forbes.com/feeds/ap/2010/03/04/business-financial-impact-mi-potato-chip-factory-explosion_7408065.html

26. *March 4, Associated Press* – (Missouri) **Leak causes 800-gallon oil spill on Missouri farm.** The Department of Natural Resources is leading the cleanup of 800 gallons of fuel on a farm in north-central Missouri. The agency was alerted March 3 of a leak from an above-ground storage tank in Randolph County. The company that owns the tank, Brownfield Oil, spread absorbent material and built a berm to contain the fuel. Officials say there is no threat to any known waterways. The contaminated soil will have to be removed and replaced.
Source: http://www.koamtv.com/Global/story.asp?S=12081621

27. *March 3, Health Day* – (National) **Food-borne illnesses in U.S. cost $152B annually.** Food-borne illnesses cost the United States an estimated $152 billion each year in health-related expenses, much more than previously thought, a new report contends. "These costs are significantly more than previous official estimates, and it demonstrates the serious burden that food-borne illness places on society," the director of the Food Safety Campaign at the Pew Charitable Trusts in Washington, D.C., said during a Tuesday press conference. Although most of these of costs are due to unidentified germs, infections from well-known pathogens play a large role. For example, costs related to campylobacter exceed $18.8 billion annually; costs linked to salmonella are estimated at $14.6 billion; and costs related to listeria are $8.8 billion, according to the report. The majority of food-borne illnesses are caused by produce, which are regulated by the U.S. Food and Drug Administration. Thirty-nine percent of E. coli outbreaks were due to produce regulated by the FDA, the report said. According to the report, California, Texas, New York, Florida and Pennsylvania have the highest costs related to food-borne illness, ranging from $6.7 billion to $18.6 billion each year.
Source: http://www.businessweek.com/lifestyle/content/healthday/636595.html

[Return to top]

Water Sector

28. *March 4, Associated Press* – (Delaware) **DNREC: 10K gallons of wastewater released.** Delaware officials say more than 10,000 gallons of wastewater has been released from Harrington's sewage treatment plant. The Department of Natural Resources and Environmental Control reported Wednesday that the lagoon at the plant on Porter Street was in danger of failing. Officials say operators were pumping the lagoon to reduce the risk of "catastrophic failure." The report did not specify what

waterway the wastewater was being pumped into.
Source: http://wjz.com/wireapnewsmd/DNREC.Harrington.sewage.2.1536458.html

29. *March 3, KCTV 5 Kansas City* – (Missouri) **Alert sent out after wastewater spill on Blue River.** A wastewater spill prompted a public alert on Wednesday. Department of Natural Resources (DNR) officials said a blocked sewer line east of U.S. 40 Highway in Kansas City resulted in 12,000 gallons of untreated sewage being dumped into the Blue River. Crews said the blockage was caused by mud from a collapsed trench. The spillage is considered a threat to public health. Once the city completes its report, the DNR will decide what steps to take next.
Source: http://www.kctv5.com/news/22732087/detail.html

30. *March 3, Water Technology Online* – (National) **Over 1,300 drinking water projects meet Recovery Act deadline.** Officials announced that all of the $6 billion allocated for drinking water and clean water state revolving funds (SRFs) by the American Reinvestment and Recovery Act was committed to signed contracts in time for the February 17 deadline, according to a press release. The Drinking Water SRF has over 1,300 project agreements signed with contracts executed, the release stated. "Not one dime had to be reallocated," said the US Environmental Protection Agency chief. Construction has begun on more than 80 percent of those projects, the release stated.
Source: http://watertechonline.com/news.asp?N_ID=73574

31. *March 2, American Progress* – (National) **Leading water utilities secure their chemicals.** More than 40 million Americans are no longer in danger of harm from a terrorist-released or accidental toxic gas plume because their water utility has converted to safer alternatives to chlorine gas in water treatment. A new survey by the Center for American Progress identifies 554 drinking water and wastewater plants in 47 states that have replaced extremely hazardous substances with safer and more secure chemicals or processes. These facilities show what can be done with proven technologies to remove chemical hazards from communities. Unfortunately, weak federal chemical security standards do not encourage more treatment plants to reduce their hazards. The Department of Homeland Security and other agencies warn that terrorists could use industrial chemicals as pre-positioned weapons. Current temporary Chemical Facility Anti-Terrorism Standards, or CFATS, exempt water utilities and do not require any facilities to look for safer and more secure chemicals and processes. And at least 2,600 additional water and wastewater facilities still use large amounts of chlorine gas. The 554 converted water facilities are located in 47 states and the District of Columbia. Of the 554 converted facilities, 235 treat drinking water, 315 treat wastewater, and four treat both. Of the 315 converted wastewater facilities, approximately 140 switched to ultraviolet light and 175 switched to liquid bleach. About two-thirds of U.S. wastewater plants already use a disinfectant other than chlorine gas, according to the U.S. Government Accountability Office. Drinking water utilities in at least 160 large U.S. cities already use liquid bleach.
Source: http://www.americanprogress.org/issues/2010/03/chemical_security.html

For more stories, see items **2** and **6**

[Return to top]

Public Health and Healthcare Sector

32. *March 4, Philadelphia Inquirer* – (Pennsylvania) **Possible prostate case error at Penn hospital.** The Hospital of the University of Pennsylvania reported a possible radiation error involving the treatment of a man for prostate cancer. On January 21, the patient underwent a prostate brachytherapy procedure to implant 65 radioactive seeds to kill cancer cells in the acorn-size gland. But when he returned for a follow-up scan on February 23, Penn doctors saw that the seeds were "outside the intended target." The incident seems to echo some of the problems at the Penn-run brachytherapy program at the Philadelphia VA Medical Center. From February 2002 until June 2008, 97 veterans got incorrect radiation doses. The January incident at Penn was reported to the state Department of Environmental Protection, which oversees the medical use of radioactive materials in Pennsylvania for the U.S. Nuclear Regulatory Commission. The report of the possible error was posted yesterday on the NRC's Web site. That report noted that the incident may have been caused by a malfunction in a new ultrasound unit, which guides the needles used to place the radioactive seeds.
Source: http://www.philly.com/philly/news/local/86311587.html

33. *March 3, Associated Press* – (National) **FDA sees increasing number of insulin pump problems.** The Food and Drug Administration said Wednesday it has seen an increasing number of hardware and software problems with insulin pumps, tiny devices worn by thousands of diabetics to deliver insulin. "Device problems critical to insulin pumps exist across manufacturers," the agency said, noting there have been 18 recalls of devices over a five-year period, including recalls by a Roche Holding AG unit and Medtronic Inc. The FDA is convening an advisory panel of outside medical experts on Friday to discuss what actions might be taken to "minimize risks associated with the devices in these recall situations." Background materials for the meeting were posted on the FDA's Web site Wednesday. The agency didn't single out specific manufacturers, which also include a Johnson & Johnson unit. Insulin pumps are primarily used by people with Type I diabetes.
Source:
http://online.wsj.com/article/SB10001424052748703862704575099961829258070.html?mod=googlenews_wsj

34. *March 3, WHTM 27 Harrisburg* – (Pennsylvania) **Man charged in bomb threat.** A 42-year-old Lemoyne, Pennsylvania, man has been arrested in connection with a bomb threat against the Medical Arts Building on the campus of Holy Spirit Hospital. East Pennsboro Township police say the man made the threat to a local radio station last week and was identified as a suspect during a review of phone records. He undergoes treatment in the Medical Arts Building and, during the phone threat, referred to himself as "The American Savior," police said. He was charged Tuesday with terroristic threats and false alarms to agencies of public safety. He was committed to Cumberland County Prison and released after posting $25,000 straight bail. A preliminary hearing was

scheduled for March 15. The February 24 threat forced the evacuation of the Medical Arts Building and the nearby Camp Hill Center for about 90 minutes.
Source: http://www.whtm.com/news/stories/0310/712190.html

[Return to top]

Government Facilities Sector

35. *March 4, Hickory Daily Record* – (North Carolina) **Bomb found at courthouse.** A bomb shaped like a coffee can, covered with duct tape and filled with gunpowder along with what look like shotgun pellets, was found in the trunk of a car at about 12:30 a.m. Wednesday morning at the Newton government center. The car, a silver Toyota Corolla, belongs ton a 43 year-old women from Newton. The woman was arrested and charged with animal cruelty on February 23 after the remains of at least six horses were found in and around a pasture she had leased. It is not known if the bomb incident is related to the animal cruelty charges, said the chief of the Newton Police Department. The bomb was found after Newton officers went to the woman's home at about 10 p.m. Tuesday in response to a report that she had been assaulted and threatened by a friend.
Source: http://www2.hickoryrecord.com/content/2010/mar/04/bomb-found-courthouse/news/

36. *March 3, KTVB 7 Boise* – (Idaho) **Students evacuated after mercury spill at Boise school.** A mercury spill caused officials to evacuate a building at Borah High Schooltheir on March 3. Fire officials say a pea-size drop of mercury spilled from a piece of jewelry worn by a student onto a desk. Several students played with the droplet before it splattered on the floor. Haz Mat crews tested 15 students, and each were determined to be OK. "I got back from lunch and there were all these fire trucks and the hazardous material truck was here," said a student. "The old gymnasium has been cordoned off and we have about five classrooms in there, one of which is that English class," said a Boise School District spokesman. Boise Fire Haz Mat crews have since cleaned up the mercury. The room has been closed and the heat turned up to evaporate any left over traces of the chemical. Boise Fire consulted experts within the Idaho Department of Environmental Quality on the clean up plans. Since the spill is so small, federal EPA crews are not being called in. Haz Mat experts will monitor the ventilation in the room and will be back at the school first thing in the morning to check out the affected classroom. If readings look normal, the classroom will be allowed to resume normal operations.
Source: http://www.ktvb.com/home/Students-evacuated-after-mercury-spill-at-Boise-school-86262367.html

37. *March 3, Lakeland Ledger* – (Florida) **No explosives found in package that led to evacuation of 10-Story building.** Officials say a suspicious package that led to the evacuation of a 10-story government building on Florida's Gulf coast was nothing explosive or suspicious. A brown bag with something inside was found propped up against a door near the Pinellas County Supervisor of Elections office at around 11:30 a.m. Tuesday. The building also contains the courthouse and other government offices.

Roads around the building were sealed off so that no vehicular traffic is allowed nearby; traffic is now flowing again.
Source:
http://www.theledger.com/article/20100303/NEWS/100309935/1374?Title=No-Explosives-Found-in-Package-That-Led-to-Evacuation-of-10-Story-Building

38. *March 3, Public Eye* – (Pennsylvania) **CISO witnesses hack like no other.** Pennsylvania's chief information security officer has seen some strange attempts to hack the commonwealth's IT systems, but none like the one he witnessed last weekend. Here is what the chief information security officer told attendees to an RSA Conference panel on state cybersecurity on Wednesday: "We saw thousands of hits on our Department of Transportation driver license exam scheduling site coming out of Russia, the same thing over and over, scheduling driver license exams. It was encrypted traffic, and we were trying to figure out what the heck is going on. Were they trying to test our systems? What exactly were they up to? The answer was, we really didn't know." Authorities eventually discovered that the hacker who used a proxy server in Russia to mask his identity owned a driving school in Philadelphia, and exploited a vulnerability in the driving test scheduling system to allow the scheduling of more tests than the allotted time slots. It could take upward of six weeks to schedule a driving test in Philadelphia. Said the chief information security officer: "What he was doing was saying [to potential customers], "You go over across the street, to John's driver training, and it's going to take you six to eight weeks to get your test. We can get you in tomorrow."
Source: http://blogs.bankinfosecurity.com/posts.php?postID=469

39. *March 3, Elk River Star News* – (Minnesota) **Bomb threat evacuates Elk River High School.** The entire Elk River High School in Minnesota was evacuated Wednesday morning after a bomb threat was made to the school. The Elk River Police Chief said at approximately 10:30 a.m. a phone call came in to the health office from an unidentified male who said something bad would happen within 20 minutes. Since this was the second threat made, the first being a written note on February 25 warning of a bombing event on March 3, school administration decided evacuation would be best. Within minutes the entire school was evacuated across the street to the Central Lutheran Church. Seven K9s from the metro area responded to the Elk River High School, and at 12:45 p.m. they were still searching the interior and exterior of the building. At this point nothing has been found. The police chief said normally when looking at events of great magnitude, like Columbine, threatening phone calls are not normally placed first. However, since it was the second threat in less than a week, the decision was made to evacuate. At this point it is unknown who made the phone call, the police chief said, however, if they are caught the will face felony charges. The Sherburne County Sheriff's Office, U.S. Marshal, and Airport Security also responded to the scene.
Source: http://erstarnews.com/content/view/11489/94/

40. *March 2, Stars and Stripes* – (International) **Tsunami warning downgraded, officials warn of high tidal swells.** Japan suffered only minor flooding and no injuries Sunday despite predictions of massive tsunami waves spawned by Chile's earthquake that

forced the evacuation of hundreds of thousands of people — including thousands of U.S. military personnel — on mainland Japan and Okinawa. Japanese officials downgraded their tsunami warning alert at about 7 p.m., but officials said there was still the possibility of 6 and 1/2-foot high tidal swells along the east coast. The off-base evacuation orders were still in effect late Sunday night. The biggest swell — at nearly four feet — occurred at 3:49 p.m. about 50 miles south of Misawa Air Base at the port of Kuji, according to the Japan Meteorological Agency. Nearly 220,000 people, including thousands of Department of Defense personnel on several U.S. base housing areas, were ordered to evacuate to higher ground on Okinawa shortly after 1 p.m., with predictions of a six-foot tsunami that officials feared would sweep over the low-lying island shortly after 3 p.m. Shortly after 5 p.m., the military residents were allowed to return to their homes after the predictions came up empty. A U.S. Marine spokesman said the evacuation of U.S. military personnel went smoothly.
Source: http://www.stripes.com/article.asp?section=104&article=68380

For more stories, see items **22**, **23**, and **43**

[Return to top]

Emergency Services Sector

41. *March 4, Honolulu Adverstiser* – (Hawaii) **5 warning sirens balk again, but 3 are returned to service.** Five emergency warning sirens that failed to work either during Saturday's tsunami scare or during Monday's monthly test were not working again yesterday during a special test. But three of the malfunctioning sirens were quickly fixed. The other two — at Sunset Beach and Ma'ili Point — were found to be damaged and will have to be repaired, said Hawaii's civil defense spokesman. In all, technicians with state Civil Defense looked at 12 sirens, and the city Department of Emergency Management inspected four others that were reported to have problems. Two sirens ended up just needing new fuses, and a third only had to have a switch turned back on.
Source: http://www.honoluluadvertiser.com/article/20100304/NEWS01/3040330/5+warning+sirens+balk+again++but+3+are+returned+to+service

42. *March 3, WREX 13 Rockford* – (Illinois) **Rockford firefighters put out flames on their own truck.** Firefighters at a Rockford, Illinois, fire station put out flames on one of their own trucks. The 1990 Ford Darley reserve fire engine suffered equipment damage and is considered a total loss worth $30,000. A sprinkler system inside the fire station helped put out the flames. Investigators believe the flames were sparked by an electrical problem.
Source: http://www.wrex.com/Global/story.asp?S=12078509

43. *March 3, Associated Press* – (Utah) **Coast Guard helicopter crashes in Utah mountains.** A Coast Guard helicopter crashed Wednesday morning in remote Utah mountains after providing security at the Winter Olympics, and three people were airlifted to local hospitals, officials said. One person was in critical condition and two

others were in serious condition, said a Wasatch County sheriff's office. Two others sustained minor injuries and were being brought out with the help of snowmobiles, he said. The HH-60 Jayhawk helicopter was one of two traveling through the area en route to home base in Elizabeth City, N.C., after performing security duty at the Vancouver Games, said a spokesman for the Coast Guard's 11th District in Alameda, California. The helicopters made a refueling stop in Salt Lake City - one of several required for the long trip - and were headed to Leadville, Colorado, when the crash occurred.
Source: http://www.forbes.com/feeds/ap/2010/03/03/general-us-helicopter-crash_7404462.html?boxes=Homepagebusinessnews

44. *March 3, Chatanooga Times Free Press* – (Georgia) **Ga. officials seek 'Blue Alert' for officers.** Local Georgia authorities say a "blue alert" bill that would notify the public if an officer is shot or killed could cut down on search time for a suspect. Senate Bill 397 is still in the Senate Public Safety Committee after the full Senate referred it back on February 10, records show. Similar to the Amber Alert law that activates to the Georgia Department of Transportation message boards when a child is abducted, the Blue Alert law would activate when a police officer has been killed or injured and the perpetrator is at large, the bill states. If enacted, the blue alert could be activated if a law enforcement agency believes the suspect has not been caught, if the suspect is believed to be a serious threat to the public and if sufficient information is available to give to the public that could assist in locating the suspect, the bill states. Law enforcement agencies already are notified when a dangerous suspect is on the loose through the National Crime Information Center powered by the FBI.
Source: http://www.officer.com/online/article.jsp?siteSection=1&id=50967

45. *March 2, Lowell Sun* – (Maine) **Maine firefighters push for marine emergency training center.** A coalition that includes Maine Maritime Academy (MMA) and the Ellsworth Fire Department is seeking federal funding to create a marine emergency training facility in the city. The group has applied for an $850,000 Port Security grant through the Department of Homeland Security to begin work on designing the facility which is planned for city-owned property in Hancock adjacent to the city's existing training center. If built, the marine emergency training facility would be one of a few such training centers in the country and the only one in the U.S. Coast Guard's Sector Northern New England which extends from Newburyport, Massachusetts, to Eastport and to the western shore of Lake Champlain. MMA provides firefighter training for its students at Ellsworth's training facility. The college also offers continuing education courses for professional mariners to update their firefighting certification. Although the city's facility has been adapted to include some maritime features, the planned training center would replicate different areas of a ship that would allow them to provide specific training in fighting shipboard fires.
Source: http://www.firerescue1.com/Firefighter-Training/articles/766295-Maine-firefighters-push-for-marine-emergency-training-center/

For another story, see item **55**

[Return to top]

Information Technology Sector

46. *March 4, V3.co.uk* – (International) **RSA 2010: Hackers using legitimate cloud services for dark ends.** Hacking groups are using legitimate cloud offerings such as Amazon Web Services to facilitate malware creation and password cracking, delegates at RSA 2010 were told. The Russian Business Network (RBN), one of the most powerful and extensive malware and hacking organisations, has been buying time on Amazon's EC2 platform to build malware and attack passwords, according to the founder of security consultancy InGuardians. The RBN, based in northern Russia, is one of the biggest and most professional hacking groups in the world. The organization started in the pornography business, but quickly moved to crime and now offers malware-as-a-service and hosting services, and provides credit card data and false identities. It is thought that one of the founders of the RBN is the son of a Russian politician, and that the group may have been behind the cyber attacks on Estonia and Georgia. Other security professionals have confirmed the use of mainstream cloud services by the hacking and malware community.
Source: http://www.v3.co.uk/v3/news/2258919/rsa-2010-hackers-legitimate

47. *March 4, IDG News Service* – (International) **Source code management a weak spot in Aurora attacks.** Companies should take extra steps to secure their source code from the type of targeted attacks that hit Google, Adobe, Intel and others over the past few months. That's according to security vendor McAfee, which released a report detailing the way software source code was accessed in some of these attacks. "We saw targeted attacks against software configuration management products," said McAfee's chief technology officer (CTO.) In many of the attacks company engineers and technical staff were targeted with malicious software. And in some cases, source code management systems were accessed and code was downloaded outside of company firewalls, the CTO said. "These systems are designed so you can have multiple people around the world working on them," he said. That often gives the bad guys several ways to get into the code. To make matters worse, source code management systems "are underprotected and not very well monitored," he said. That means that they could make easy targets in future attacks.
Source:
http://www.computerworld.com/s/article/9165718/Source_code_management_a_weak_spot_in_Aurora_attacks

48. *March 4, The Register* – (International) **Hacking human gullibility with social penetration.** Two security penetration testers rely plenty on attacks that exploit weaknesses in websites and servers, but their approach is better summed up by the famous phrase "There's a sucker born every minute". That's because so-called social penetration techniques are more reliable and easier to use in identifying chinks in client fortresses, the principals of Mad Security said on March 3. That's true even for organizations that place a high premium on security and train their employees to resist the most common attempts to trick them into letting down their guard. One of the testers said he regularly sends client employees emails informing them the strength of their login passwords is being tested through a new website. They are then instructed to

follow a link and enter their credentials. The success rate: as high as 50 percent. The vulnerability stems from humans' inherent tendency to trust one another.
Source: http://www.theregister.co.uk/2010/03/04/social_penetration/

49. *March 4, Help Net Security* – (International) **RSA authentication weakness discovered.** The most common digital security technique used to protect both media copyright and Internet communications has a major weakness, University of Michigan computer scientists have discovered. RSA authentication is a popular encryption method used in media players, laptop computers, smartphones, servers and other devices. Retailers and banks also depend on it to ensure the safety of their customers' information online. The scientists found they could foil the security system by varying the voltage supply to the holder of the "private key," which would be the consumer's device in the case of copy protection and the retailer or bank in the case of Internet communication. It is highly unlikely that a hacker could use this approach on a large institution, the researchers say. These findings would be more likely to concern media companies and mobile device manufacturers, as well as those who use them. A doctoral student in the Department of Electrical Engineering and Computer Science will present a paper on the research at the upcoming Design, Automation and Test in Europe (DATE) conference in Dresden on March 10.
Source: http://www.net-security.org/secworld.php?id=8969

50. *March 3, Network World* – (International) **Wi-Fi could lead thieves right to your laptop.** Stuffing a company laptop into the car trunk or even a locker, without turning off its Wi-Fi radio, can be an open invitation to thieves, according to Credant Technologies. Thieves with increasingly sophisticated, directional Wi-Fi detectors can home in on the laptop's radio, tracking it down even when the PC is hidden away. A statement by the mobile security software vendor highlighted a recent warning from a security specialist at University of Technology, in Jamaica. He said that it appeared crooks running a lottery scam on the island were using stolen laptops to do so. They tracked down the often out-of-sight computers using Wi-Fi radio detectors. The detectors, sometimes called "Wi-Fi finders," are readily and inexpensively available. But many of them simply register the presence and strength of Wi-Fi signals, such as those from public hotspots. Depending on the features, the detector may not be very helpful in finding a precise location, for example, an active laptop radio in an automobile parked with a lot of others. But Hawking Technologies' Hi-Gain WiFi Locator Professional Edition includes a high-gain antenna that can more precisely locate a Wi-Fi radio.
Source:
http://www.pcworld.com/article/190674/wifi_could_lead_thieves_right_to_your_laptop.html

51. *March 2, PC World* – (International) **Digital thieves dominate data breaches.** For the first time, hackers have become the biggest cause behind publicly reported data breaches, according to a recent report. The Identity Theft Resource Center began tracking the cause of reported breaches three years ago. For the past two years, the top cause was what the ITRC calls "data on the move"—typically a lost laptop with

unencrypted data, or even a lost briefcase. That changed in 2009, when about one out of every five data breaches had a hacker behind it. A thief who walks away with a laptop is likely more interested in wiping its hard drive and selling it than in selling its data. But a hacker who invades a company's network and swipes a trove of credit card numbers is sure to use them, or sell them to someone else who will. The ITRC notes that its study is based only on reported breaches. Because state laws and policies vary, not all breaches or their causes are reported. The number of data breaches dropped from 657 in 2008 to 498 in 2009 (in 2007, there were 446). But the while the total number of breaches dropped, the number of hacker-launched thefts rose.
Source: http://www.computerworld.com/s/article/9164280/Digital_Thieves_Dominate_Data_Breaches

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

52. *March 4, WBAY 2 Green Bay* – (Wisconsin) **WBAY transmission line repair to be in mid-spring.** WBAY-TV's chief engineer says WBAY's transmission line will be replaced in late April or early May. The entire, multi-ton transmission line which has many components needs to be replaced. Delivery of the parts for the repair is now expected in late April, and coordinating the extensive repair job will take several days after the delivery. In January, WBAY-TV experienced a power drain in its over-the-air signal. The engineer says when crews examined the transmission line at WBAY-TV's broadcast tower, they discovered damage from a "flashover" inside the line. WBAY-TV is transmitting with as much power as possible without risking further damage. Arrangements were made to provide WBAY's signal by ground cables to cable companies, AT&T U-Verse, and Dish Network, and WBAY's signal is still reaching 96 percent of WBAY's viewing audience compared to before experiencing transmission problems.
Source: http://www.wbay.com/Global/story.asp?S=12077929

53. *March 3, Asheville Citizen-Times* – (North Carolina) **WNCW knocked off the air today, but remains online.** Public radio station WNCW-FM/88.7 has been temporarily knocked off airwaves, but continues to operate today via the Internet. The station is experiencing "major technical issues" at its transmitter site on Clingman's Peak, and a repair crew is on the way to fix the problem, according to an announcement posted on the station's web site. The station's programs continue to stream online at

www.wncw.org
Source: http://www.citizen-times.com/article/20100303/ENT/100303025/1005/ENT

54. *March 3, Federal Computer Week* – (National) **DOD's reliance on commercial satellites hits new zenith.** The U.S. military is increasingly turning to the private sector for many of the services it relies on. After the supply of energy and terrestrial fiber communications, satellite communications is the top capability that the U.S. military relies on the private sector to deliver. Industry experts estimate that 80 percent of all satellite bandwidth that the Defense Department uses is purchased by the Defense Information Systems Agency from companies such as Inmarsat, Intelsat and Iridium. That percentage is expected to climb north of 90 percent in the near future as unmanned aerial vehicles and other intelligence, surveillance and reconnaissance (ISR) systems begin transmitting in high definition, which will require even more bandwidth. New satellite constellations, such as the Mobile User Objective System (MUOS), are expected to take up some of the slack. However, the need for supplemental bandwidth is expected to continue growing during the time that the five MUOS satellites are put into orbit between 2010 and 2015. DOD leaders might have legitimate concerns about the department's dependence on the private sector for such a vital tactical capability.
Source: http://fcw.com/articles/2010/03/03/cover-story-the-satcom-challenge.aspx

[Return to top]

Commercial Facilities Sector

55. *March 4, Petoskey News-Review* – (Michigan) **City arranges public safety evaluation.** Petoskey officials have enlisted a consultant to review the city's delivery of public safety services. The evaluation is expected to yield some recommendations for how fire and police protection might be provided along the Bay Harbor resort corridor. A senior public safety consultant with the International City/County Management Association will be in Petoskey to conduct the review on March 8 and 9. The Bay Harbor resort was brought into Petoskey's jurisdiction through a 1994 municipal transfer agreement. In recent years, numerous Bay Harbor property owners have voiced a desire to have emergency services available closer to the resort. The far western reaches of Bay Harbor are more than 7 miles from the city's existing fire station on Lake Street.
Source: http://www.petoskeynews.com/news/article_3e67e954-2796-11df-812e-001cc4c002e0.html

56. *March 3, WPDE 15 Florence* – (South Carolina) **Public safety training for a MB terrorist attack.** Wednesday was day three of a four-day public safety training exercise hosted in Myrtle Beach, South Carolina, where first responders from all over the southeast prepare for the worst. First responders, from as far as Kentucky and Alabama and as close as Myrtle Beach and Horry County prepared for the worst - a chemical terrorist attack on a Grand Strand beach. If the worst was to happen, each agency would have a role. "What we try to do is identify the unknown. In today's scenario, some kind of agent has been used against the folks on the beach, so it's our job to take a sample of

that, take into our mobile lab and analyze it," illustrated a Lieutenant Colonel with the North Carolina National Guard.
Source: http://www.carolinalive.com/news/story.aspx?id=424747

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

57. *March 4, Natchez Democrat* – (Louisiana) **Officials: Stay off the levee.** Wet or dry, but especially when wet, stay off the levee. That is the message officials with the Louisiana Fifth Levee District want to get out. "The levees are in good shape, the Mississippi River has been on the drop, but our main problem is getting people to stay off of them, to keep them from rutting them up," said a Fifth District Levee Board member who lives in Ferriday. The Mississippi River reached 49.1 feet in mid-February — flood stage at Natchez is 48 feet — and is currently falling, predicted to continue a downward trend. It is expected to stand at 41 feet the morning (March 4). "We are thankful the river is falling like it is, and it continues to fall, but we are yet to see the spring rains," the Fifth Levee District president said. And that is why it is important to stay off of the levees, said a levee district board member from Monterey. "Any kind of activity up and down the levees, four-wheelers or anything that would cut ruts, any four-wheel drives, any kind of destruction of the levee is illegal," he said. Rutting the levees not only make it hard for the levee district to continue surveying the levees during high water, but he said they can actually harm the structural quality of the levees. He said that the fine for levee damage is whatever it costs to repair the levee, and that one man last year spent time in jail because he wasn't able to pay the $3,500 fine. "The levees are protecting everybody in here, so (people) should just use common sense about what they are doing," he said.
Source: http://www.natchezdemocrat.com/news/2010/mar/04/officials-stay-levee/

58. *March 2, Burlington Times News* – (North Carolina) **Burlington dams need $9.1 million in repairs.** Structural impairments at two Burlington, North Carolina, dams will force the city to pay about $9.1 million in repairs by 2012, officials said Tuesday. Paying for the repairs will require a 2-percent increase in Burlington's water and sewer bills over three years, equaling about 60 cents per month in raised rates on the average bill. Dams at Stoney Creek and Lake Cammack could not withstand major flood events they were originally designed to handle, the Burlington Water Resources Director said Tuesday. A 300-year flood would likely cause the dams to break, flooding areas downstream. At Stoney Creek, flooding rains cause overflows around the dam, eroding abutments there and increasing the likelihood of dam failure. At Lake Cammack, a chemical reaction in the concrete is weakening the dam and abutments at the dam are

not high enough, inspectors found. Stoney Creek Dam will cost about $6.4 million to repair by drilling and running cables vertically through dam into the bedrock below, anchoring the structure and protecting against water pressure. Concrete walls will be extended horizontally into the earth around the dam, keeping river banks and abutments from eroding during floods and protecting Burlington's reservoir. Lake Cammack Dam will cost about $2.7 million to repair by elevating earthen abutments beside the dam and using cables to anchor the dam. Bidding and construction will likely happen in the spring and summer of 2011.
Source: http://www.thetimesnews.com/news/burlington-32063-repairs-million.html

For another story, see item **28**

[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