Homeland Security

Daily Open Source Infrastructure Report for 28 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 Examiner, Toyota announced Tuesday that it is suspending sales of eight models that are involved in the recall for having accelerator pedals that stick. In addition to the sales freeze, production at certain Toyota facilities will pause beginning the week of February 1. (See item **10**)
- The Associated Press reports that Chattanooga, Tennessee officials fixed a Tuesday morning power failure at the Moccasin Bend wastewater plant that released 137 million gallons of sewage and stormwater into the Tennessee River. (See item **31**)

Fast Jump Menu

PRODUCTION INDUSTRIES
- Energy
- Chemical
- Nuclear Reactors, Materials and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SUSTENANCE and HEALTH
- Agriculture and Food
- Water
- Public Health and Healthcare

SERVICE INDUSTRIES
- Banking and Finance
- Transportation
- Postal and Shipping
- Information Technology
- Communications
- Commercial Facilities

FEDERAL and STATE
- Government Facilities
- Emergency Services
- National Monuments and Icons

Energy Sector

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

1. *January 27, Denver Post* – (Colorado) **Xcel's Pueblo plant faces stiffer limits on mercury.** Xcel Energy's new $1 billion Comanche 3 power plant near Pueblo, slated to come on line February 19, will face stiffer limits on emissions of toxic mercury. But an attempt to get a federal court order to stop the coal- fired plant until a permit is issued was rejected on January 26. U.S. district court judge denied a temporary restraining

order requested by the environmental group WildEarth Guardians. He, however, left the suit pending. The new permit — which will cut the permissible amount of mercury by about 25 percent — should be issued in two to six weeks, said the director of the state Air Quality Control Divisions. Based on analysis of comparable plants, the director said the new standard was "stringent." In 2005, the state issued a permit requiring the plant to capture about 65 percent of the estimated 377 pounds of mercury the plant could emit annually. Since then, the federal requirements have changed, and the new permit requires capture of more than 80 percent. "We think we will be able to meet the permit limits," an Xcel spokesman said. Mercury can damage the nervous system, and fish in 20 percent of Colorado's lakes and reservoirs have been found to have elevated levels. The 750-megawatt Comanche 3 unit was originally scheduled to go on line in November, but leaking steam tubes in the boiler have repeatedly delayed the startup. "We got up to 47 percent capacity last week and found a couple of more leaks," the spokesman said.
Source: http://www.denverpost.com/headlines/ci_14274031

2. *January 26, Marietta Times* – (Ohio) **2 accused of cutting power lines.** Two West Virginia men arrested Friday in Lowell for cutting power lines in order to steal copper wiring may have done something similar in Meigs County recently, said a Washington County Sheriff. One man, 37, and another man, 29, both of Chapmanville, West Virginia, were arrested on January 22 and charged with felony counts of theft, possession of criminal tools and disrupting public service. They remained in jail on January 25. The men were allegedly cutting power lines along Ohio 60 in the early morning hours on January 22 and were found covered in mud, in possession of tree trimmers and with differing stories about why they were in Lowell, according to deputies. "They were stealing copper," said the sheriff. "They had purchased a couple long-limb tree trimmers and had put tape and things around them to ward off electric shocks as they cut the lines." He said the two are suspects in another recent case. "We knew at least 4,000 feet of wire was taken in Meigs County," he said. "We believe it's attributable to the same people." An AEP spokesman said the company will have to pay about $20,000 to replace the lines that were cut. Power was out from 2:32 a.m. on January 22 until 5:41 a.m. for 72 customers, he said. "We put a temporary fix in place, but we'll have to rebuild," the spokesman said. He said a recent incident in Pomeroy, in Meigs County, also involved AEP lines.
Source: http://www.mariettatimes.com/page/content.detail/id/519045.html

3. *January 26, KRIV 26 Houston* – (Texas) **Hangman's noose found at BP plant in Texas City.** BP officials say a hangman's noose was found at one of their Texas City refinery units, and they are offering a $10,000 reward to anyone who identifies the person responsible for it. The noose was discovered last month at a resid hydrotreating unit, which refines crude oil into fuel, the refinery's manager wrote in a memo sent to employees on January 22. The manager continued to write that hangman nooses are symbols of hatred and violence. BP officials are now investigating the incident, he wrote. The person behind the noose will be banned from the building, or terminated if the person is an employee of the company, he wrote.
Source: http://www.myfoxhouston.com/dpp/news/local/100126-bp-hangmans-noose

4. *January 26, KUSA 9 Denver* – (Colorado) **Leadville explosion started by leaking fuel tank.** Investigators say a damaged fuel tank started a series of explosions that destroyed a former Coca-Cola bottling plant on Friday afternoon, sending four people to the hospital. The first explosion happened just after 3 p.m., setting fire to the building and collapsing more than half of it in the blast. Firefighters rescued men who were trapped inside. One had to be airlifted to a Denver hospital, but is expected to be OK. The other three were treated and released for smoke inhalation. Investigators say the fire started in one of the businesses housed in the building called Gas Consultants and was an accident. There is no evidence of criminal activity, according to authorities. Only one business, Millenium Towing, was not destroyed by the fire. Investigators say employees at AG Masonry will be able to salvage some of their equipment. Four other businesses were also in the building. It took crews nearly seven hours to put out the fire.
   Source: http://www.9news.com/news/local/article.aspx?storyid=131542&catid=346

5. *January 25, KSFY 13 Sioux Falls* – (South Dakota) **Thieves steal $20,000 from power crew staying at Sioux Falls hotel.** Sioux Falls Police say a Mississippi electric crew who were on their way to North Dakota to help restore power, lost as much as 20-thousand dollars in tools, after they were robbed at their hotel. Police say boom trucks from Chain Electric were sitting in the parking lot of the Holiday Inn Express on South Shirley Avenue, when the tools were stolen. No arrests have been made.
   Source: http://www.ksfy.com/news/local/82620837.html

6. *January 25, Associated Press* – (Oregon) **4 Ore. men sentenced for shooting power lines.** Four young Linn County, Oregon, men have been sentenced to five years probation after pleading guilty to shooting down high-voltage power lines near McDowell Creek Park in the Lebanon area. They were also ordered to pay more than $13,000 in restitution to the Bonneville Power Administration for the December 2008 destruction of government property. The U.S. attorney's office says the men shot a .22 caliber rifle at ceramic insulators attached to a large transmission tower that held several high voltage power lines supplying electricity to the Lebanon area. The gunfire shattered three insulators, downing a major electrical line, and causing an 80-minute power outage to thousands of customers. Sentenced on January 25 in federal court in Eugene were a 24-year-old, a 19-year-old, a 20-year-old, and a 25-year-old.
   Source: http://www.ktvz.com/Global/story.asp?S=11879614

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials and Waste Sector

7. *January 27, San Luis Obispo Tribune* – (California) **Diablo Canyon Power Plant faulted for not testing valves for months.** A failure to conduct proper testing caused two safety valves to be misaligned for more than a year at Diablo Canyon nuclear power plant. That is the conclusion of a special inspection conducted by the Nuclear Regulatory Commission just after Thanksgiving. The inspectors and other agency officials met with plant operators Tuesday to discuss the results at a public meeting. In February 2008 during a previous refueling outage, operators at the plant made several modifications to valves that would be used to recirculate cooling water lost from the reactor resulting from a broken pipe or other severe accident, said a senior resident NRC inspector at the plant. The modifications prevented two valves from being opened remotely, but this was not discovered at the time because of a lack of testing. The top executive at the plant said procedures are now in place to ensure that needed testing will be done. "We take this issue very seriously," he said.
Source: http://www.sanluisobispo.com/news/local/story/1005099.html

8. *January 26, Salt Lake Tribune* – (Utah) **Public largely critical of depleted uranium disposal.** On Tuesday, some Utahns said radioactive waste does not belong in a shallow disposal site in western Utah. The Utah Division of Radiation Control's public hearing on a proposed regulation for depleted uranium attracted more than three dozen people. EnergySolutions says it already has buried about 49,000 tons of depleted uranium at its mile-square disposal site 80 miles west of Salt Lake City. And one of three controversial shipments (totaling another 11,000 tons) awaits disposal from the government cleanup of the Savannah River atomic-bomb site in South Carolina. But, before any more of the nation's 700,000-ton stockpile of depleted uranium comes to Utah, state regulators want to finish a regulation to require the Salt Lake City nuclear waste company to prove the site is right for the waste. The company's study would have to show that the state's safety requirements can be met for at least 10,000 years and also predict how well the site will hold up when the depleted uranium becomes most dangerous.
Source: http://www.sltrib.com/news/ci_14275000

[Return to top]

Critical Manufacturing Sector

9. *January 27, Reliable Plant Magazine* – (Connecticut) **Conn. plant faces fines for fire and explosion hazards.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has cited Fibrelite for 21 alleged violations of workplace safety standards at its Pawcatuck, Connecticut plant. The manufacturer of composite manhole covers faces a total of $90,500 in proposed fines, chiefly for potential fire and explosion hazards. OSHA's inspection found that combustible particulate solids, which were generated during trimming and repair operations, were not collected into an adequately designed dust collection system, were allowed to accumulate on machinery and surfaces, and were not adequately cleaned up to prevent such buildup. The combustible material was exposed to several potential ignition sources, including an LP gas-powered industrial truck, exposed wiring and a spark

producing tool. Other hazards identified during OSHA's inspection include improper storage of waste material saturated with combustible residue, flammable liquid waste allowed to drip into an open bucket, inadequate precautions to avoid ignition sources for flammable liquids, a spray booth lacking a sprinkler and adequate grounding, a lack of an emergency action plan, unguarded power presses, a lack of specific energy control procedures for various machines, excess air pressure for a cleaning hose and several electrical hazards. These conditions resulted in Fibrelite being issued 20 serious citations with $89,500 in fines. The company also has been issued one other-than-serious citation, with a $1,000 fine, for incorrectly recording injuries and illnesses.
Source: http://www.reliableplant.com/Read/22458/Connecticut-plant-faces-fines

10. *January 26, Examiner* – (International) **No sale: Toyota halts sales of eight models, production affected as well.** Toyota announced Tuesday that it is suspending sales of eight models that are involved in the recall for having accelerator pedals that stick. Initially Toyota had maintained that improperly installed floor mats were to blame, but as time has continued on, the company has recently admitted that "Certain accelerator pedal mechanisms may, in rare instances, mechanically stick in a partially depressed position or return slowly to the idle position." One driver of a Toyota Avalon was able to use information circulated by the media, moving the car's shifter to and from neutral, to limp his malfunctioning car to a dealership while it was still experiencing the acceleration issue. The service manager was able to verify that the floor mat was not obstructing the accelerator. Toyota now hopes to show that it is taking ownership of the issue and is acting in the best interest of its customers. Models impacted by the sales freeze include the following: 2009-2010 RAV4, 2009-2010 Corolla, 2009-2010 Matrix, 2005-2010 Avalon, 2007-2010 Camry, 2010 Highlander, 2007-2010 Tundra, and 2008-2010 Sequoia. In addition to the sales freeze, production at certain Toyota facilities will pause beginning the week of February 1. Facilities in question include: Toyota Motor Manufacturing, Canada (Corolla, Matrix, and RAV4), Toyota Motor Manufacturing, Indiana (Sequoia and Highlander), Toyota Motor Manufacturing, Kentucky – Line 1 (Camry and Avalon), Subaru of Indiana Automotive, Inc. (Camry), Toyota Motor Manufacturing, Texas (Tundra). At this point, Toyota is not indicating how long the sales and production suspension will last.
Source: http://www.examiner.com/x-10697-California-Autos-Examiner~y2010m1d26-No-sale--Toyota-halts-sales-of-eight-models-production-affected-as-well

For more stories, see items **24** and **30**

[Return to top]

Defense Industrial Base Sector

11. *January 27, Lompoc Record* – (California) **Missile-defense test scheduled for VAFB.** A missile-defense system test set for Sunday at Vandenberg Air Force Base will involve a different scenario, this time gauging how the system would react to an Iran-like attack, officials said. The test, which will occur Sunday afternoon, will involve a target weapon set to take off from the Kwajalein Atoll, about 4,200 miles

southwest of Vandenberg. That launch will be followed about 20 minutes later by a ground-based interceptor launched from an underground silo on north Vandenberg. During an interview with Reuters news service reporters last month, the Missile Defense Agency director said the scenario would involve "a class of long-range missile technology we might expect in the future from a country like Iran, as well as from a country like North Korea." The approximately $120 million test marks the first time for a target to be launched from Kwajalein when the interceptor is launched from Vandenberg, a spokesman noted. While the complexity of the test is "generally the same" as any others, this will involve "more of a head on intercept vs. more from the side as in previous tests," the spokesman added.
Source: http://www.lompocrecord.com/news/local/military/article_8c15b286-0b11-11df-9bd6-001cc4c002e0.html

12. *January 27, Space-Travel.com* – (National) **Alternate space capsule concept passes tests.** A NASA team looking into design concepts for future space capsules has successfully demonstrated that an all-composite structure is a feasible alternative to traditional metal capsules for carrying astronauts into space and returning them safely to Earth. These advanced composite materials promise potential benefits over traditional metal structures, such as being easily formed into complex shapes that may be more structurally efficient. A NASA team developed and tested the capsule in a series of full scale structural tests. The full-scale crew module was pressurized to design limits while critical interfaces were pulled to simulate the combined loads a future crew module might see during launch and return to Earth. Follow-on tests checked for damage tolerance, a question of critical importance for composite structures. At points along the way, the damaged sites were inspected by non-destructive means, using both infrared thermography and ultrasonic techniques, to characterize subsurface damage and damage progression. "We are very pleased with the entire test series. Throughout testing, there were no anomalies and performance aligned amazingly well with analytical predictions," the program manager said. The composite crew module was designed, manufactured, inspected and tested in a collaborative partnership between NASA and industry. Partners include subject matter experts from nine of ten NASA centers, the Air Force Research Laboratories, Alcore Corporation, Alliant Techsystems (ATK), Bally Ribbon Mills, Collier Corporation, Genesis Engineering, Janicki Industries, Lockheed Martin and Northrop Grumman.
Source: http://www.space-travel.com/reports/Alternate_Space_Capsule_Concept_Passes_Tests_999.html

[Return to top]

Banking and Finance Sector

13. *January 27, IDG News Service* – (International) **3D secure online payment system not secure, researchers say.** A widely deployed system intended to reduce on-line payment card fraud is fraught with security problems, according to University of Cambridge researchers. The system is called 3-D Secure (3DS) but known better under the names Verified by Visa and MasterCard SecureCode. Implemented and paid for by

e-commerce vendors, the systems require a person to enter a password or portions of a password to complete an on-line purchase. As a reward for investing in the systems, merchants are less liable for fraudulent transactions and are stuck with fewer chargebacks. But banks such as the Royal Bank of Scotland are now holding consumers to a higher level of liability if fraudulent transactions occur using either system, said a security researcher at the University of Cambridge. That is despite what the researcher and a security engineering professor contend are several flaws with 3DS. One of their main points is how 3DS is integrated into Web sites during a transaction. E-Commerce Web sites display 3DS in an iframe, which is a window that brings content from one Web site into another. The e-commerce Web site connects directly to a bank, which solicits a person's password in the iframe. If the password is right, the transaction is complete. But the researchers argue that since there's no URL displayed with the iframe, it's difficult to tell whether it's genuine or not. 3DS also allows people to set their password immediately as they enroll in the system, a process called "activation during shopping" (ADS). The ADS enrollment will ask for some other piece of information, such as a birth date, in order to confirm the setting of the password. That's a security issue since birth dates are easily obtainable, the researchers argue.
Source:
http://www.pcworld.com/businesscenter/article/187849/3d_secure_online_payment_system_not_secure_researchers_say.html

14. *January 27, Courthouse News Service* – (National) **FDIC seeks comments on risk in employee pay.** The Federal Deposit Insurance Corporation (FDIC) is requesting comments regarding whether it should penalize insured institutions with higher Deposit Insurance Fund (DIF) assessments when it determines they have risky employee compensation plans. The FDIC maintains that it is not attempting to eliminate any particular compensation plan through increased rate assessment but it does recognize the "broad consensus that some compensation structures misalign incentives and induce imprudent risk" by rewarding "...employees based on short-term results without full consideration of the longer-term risks to the firm." The Federal Deposit Insurance Act requires that a depository institution's deposit insurance assessment must be based on the probability that the DIF will incur a loss, the amount of any loss, and the revenue needs of the DIF. In 2009 employee compensation plans were cited as a contributing factor in an institution's failure in 35 percent of the agency's investigations. The agency hopes that using assessment rates will provide incentives for insured institutions to adopt compensation programs that align employees' interests with those of the institution's other stakeholders. According to the agency, such compensation plans would limit stock awards to restricted, non-discounted companies that would be available at intervals over a period of years after an employee meets multi-year performance goals. The agency also believes that any cash bonuses or stock awards should be subject to so-called "clawback" provisions in case the performance a bonus is based on later proves to have been illusory or deceptive.
Source: http://www.courthousenews.com/2010/01/27/Federal_Regulations.htm

15. *January 27, Bank Info Security* – (National) **Phishing trends: numbers up, corporate accounts targeted.** The latest report from the Anti Phishing Working Group (APWG) paints a distressing picture for anyone doing transactions online, says the chairman of the APWG. All phishing numbers are on the rise. The number of unique phishing reports submitted to APWG for the third quarter of 2009 reached a record 40,621 in August — 10 percent more than the previous record set in September 2007. "What we are all seeing is that the criminals are still continuing their attacks and it is getting worse," the chairman says. "They're getting way more sophisticated." The number of unique phishing websites reached a record 56,362 in August, displacing the previous reported high of 55,643 in April 2007. The number of hijacked brands rose to a high of 341, up more than 10 percent from the previous record of 310 in March 2009. What really worries the chairman is the targeting of corporate bank accounts and high-wealth customers, as well as the circumvention of authentication technology. "These criminals are rapidly figuring out how the financial industry works, where there is big money and large transfers, so they can basically do large wires out of these accounts without setting off fraud alerts." The chairman says bluntly, "I think we're in for a challenging year." He's heard from banks telling him it is a hostile environment. "They're scrambling for answers to this because they just can't be everywhere the hackers are — even on the users' computers."
Source: http://www.bankinfosecurity.com/articles.php?art_id=2119

16. *January 27, Mississippi Press* – (Mississippi) **Debit card scam: Local banks want customers to beware of account draining phone call.** Officials with two local banks warned on January 26 of a debit card scam that could drain a person's banking account if they follow the recorded instructions. The senior vice president of security at Merchants & Marine Bank said several of the bank's customers reported on January 25 and 26 of receiving a recorded call on their cell phone telling them their Visa debit bank card is restricted or inactive. The recording tells them that in order to reactivate the card they should put the card's account number into the telephone key pad, the vice president said. The communications director at Hancock Bank said their customers have reported receiving the same recorded call. The chief of investigations with the Jackson County Sheriff's Department said unfortunately as technology advances, bank account scams tend to evolve. A customer service representative at M&M Bank said her customers are saying that the calls are coming from two different phone numbers in Tennessee. The chief of investigations said the calls are most likely coming from a "drop box" that routes calls several places, making it nearly impossible to trace.
Source: http://blog.gulflive.com/mississippi-press-news/2010/01/debit_card_scam_local_banks_want_customers_to_beware.html

17. *January 27, St. George Spectrum* – (California) **Credit union issues warning after fraud trend in California.** Southwest Community Federal Credit Union has issued a fraud alert to its customers after reports some Visa accounts have been targeted by thieves in California. "We've basically put a block on all transactions out of California. That includes legitimate transactions, which is the majority of the transactions," the chief financial officer said on January 26. An alert posted on the company's Web site said the credit union initiated the statewide block after spotting the trend, and credit

union members who are traveling to California or doing online business with companies based in California will need to contact Southwest Federal for assistance in clearing the transaction. Once Southwest Federal is able to authenticate the credit union member's identity, the transactions will be allowed. The chief financial officer said the California blockade will eventually be lifted once the credit union deems it safe to do so. Skilled thieves are selling and buying black market equipment that allows them to reproduce debit and credit cards with a great deal of accuracy, he said. The fraud trend in question is called a "card present transaction." In other words, the transactions are not taking place on the Internet where a PIN number would be required to complete the transaction. Instead, the alleged thieves are presenting the phony cards along with false identification, and then signing for their purchases.
Source:
http://www.thespectrum.com/article/20100127/NEWS01/1270312/Credit+union+issues+warning+after+fraud+trend+in+California

18. *January 26, Computerworld* – (Texas) **Bank sues victim of $800,000 cybertheft.** A Texas bank is suing a customer hit by an $800,000 cybertheft incident in a case that could test the extent to which customers should be held responsible for protecting their online accounts from compromises. The incident, which was first reported by a blogger this week, involves Lubbock-based PlainsCapital bank and its customer Hillary Machinery Inc. of Plano. In November 2009, unknown attackers based in Romania and Italy initiated a series of unauthorized wire transfers from Hillary's bank accounts and depleted it by $801,495. About $600,000 of the amount was later recovered by PlainsCapital. Hillary demanded that the bank repay it the rest of the stolen money. In a letter to the bank in December, Hillary claimed that the theft happened only because PlainsCapital had failed to implement adequate security measures. PlainsCapital promptly filed a lawsuit in the U.S. District Court for the Eastern District of Texas asking the court to certify that its security procedures were "commercially reasonable." In its complaint, the bank noted that it had made every effort to recover the stolen money. The bank sought to absolve itself from blame in the heist by stating that the unauthorized wire transfer orders had been placed by someone using valid Internet banking credentials belonging to Hillary Machinery. "PlainsCapital accepted the wire transfer orders in good faith" and had therefore not breached any of its agreements with Hillary, the bank said in its complaint. The complaint itself is somewhat unusual in that it does not seek anything specific from Hillary. Rather, all it asks is for the court to certify that its systems are reasonably secure.
Source:
http://www.computerworld.com/s/article/9149218/Bank_sues_victim_of_800_000_cybertheft

19. *January 26, Oil Express* – (Kansas) **Thieves empty jobber's ATM using factory default pin.** A scam involving factory pre-set PIN numbers for ATMs has cost a Kansas marketer the contents of his cash dispenser in a matter of seconds, Oil Express reports. The marketer, who never changed the ATM's original code, said the loss was preventable. "If we had just read the manual that came with the ATM, we would have known to change the code, but we didn't," he said. Oil Express reports the theft could

signal a trend, as marketers buy and sell stores and inherit older ATMs. "We would advise anyone with a legacy ATM that's more than five years old to check whether the PINs were ever changed and to make sure that they have the test software installed," said a spokesman for ATM manufacturer Triton told the news source. ATM vendors offer free software that helps prevent ATM thefts. New ATMs contain a PIN that allows owners to access the machine's menu. While it does not provide access to the cash vault, it does allow thieves to change the denomination of the bills that the ATM dispensed. In the Kansas case, while the manager loaded the ATM with $20 bills, the thieves, accessing the ATM menu, changed the denomination of the bills to $1. As a result, the thieves received 20 times the amount that the ATM actually calculated that it had dispensed. ATM vendors learned of the scam several years ago. As a result, machines manufactured today force operators to change the PIN before the machine can be used. However, the older systems are still vulnerable, the reason that Triton and other vendors produced a free software fix.
Source: http://www.nacsonline.com/NACS/News/Daily/Pages/ND0126101.aspx

20. *January 26, Associated Press* – (Michigan) **Burglars take more than $9,000 from Treasury safe.** The State of Michigan is looking at a possible $2 billion deficit in the fiscal year starting October 1, and the theft of more than $9,000 from a branch office is not helping. Sterling Heights police tell the Detroit Free Press that employees reporting to work on January 25 discovered the theft. It is believed to have occurred between 4:30 p.m. on January 23 and 6:30 a.m. January 25. Police say the thieves broke a window and removed part of a wall to get into a room where a safe was forced open. A Treasury spokesman says the field office and collection staffers work at the suburban Detroit location, where back taxes, state agency debt and other payments can be made. He says the office will remain closed until repairs are completed, possibly by the end of the week.
Source: http://www.chicagotribune.com/news/chi-ap-mi-treasuryoffice-th,0,168115.story

21. *January 26, Queens Courier* – (New York) **Phony bomb bank robberies.** Two recent bank robberies have taken advantage of terrorism fears in northeast Queens, and police want to defuse the situation. On January 22 a "black male, 5 feet 11 inches tall, weighing approximately 200 pounds," according to the NYPD, entered the Queens County Savings Bank at 247-53 Jamaica Avenue in Bellerose shortly before 9 a.m. Police say the man, dressed in black shoes and a black jacket, told bank employees he wanted to open an account. Once he had the manager's attention, cops say he said he had a bomb in his bag, and warned them "Don't notify anyone." He fled the bank with an undisclosed amount of cash, heading westbound on Jamaica Avenue. Police sources told The Queens Courier that on January 25, an unidentified black male, between 6 feet and 6 feet 2 inches tall, weighing "about 180 pounds," entered the Queens County Savings Bank at 224-04 Union Turnpike in Hollis Hills shortly before noon on. The man, who was wearing blue pants, a blue trench coat and black sneakers, also produced what appeared to be a bomb — but also turned out to be four traffic flares taped together with a common electronic accessory, police sources said. The thief was last seen headed south on Springfield Boulevard, with approximately $8,300 in cash,

according to police sources.
Source:
http://www.queenscourier.com/articles/2010/01/26/news/regional/northeast/doc4b5f7a16df89d736102907.txt

22. *January 26, eCredit Daily* – (International) **Report: 'Credit card twitter' ripe for phishing attacks.** Blippy, the 'Twitter' for credit card users that went live this month, could be targeted by cyber criminals that could use the personal information posted on the social media site to create effective phishing emails, according to a prominent cyber security firm. Blippy invites users to discuss what they are buying primarily by attaching a credit or debit card to the service. Postings reveal what they purchased, the amount and the retailer, whether online or in-store. ATM withdrawal amounts are also recorded. The site has privacy safeguards in place, but there is enough revealed in the postings to help cyber fraudsters construct phishing schemes aimed at Blippy users, according to Cyveillance, a provider of online security solutions to protect organizations from cyber attacks, including phishing and malware. The firm has done business with a majority of Fortune 500 companies. "From a cyber criminal's point of view, Blippy currently offers great information to construct a highly-targeted spear phishing attack," Cyveillance writes on its cyber intelligence blog.
Source: http://ecreditdaily.com/2010/01/report-credit-card-twitter-ripe-phishing-attacks/

23. *January 26, Bank Info Security* – (Texas) **ATM Fraud: Skimming scheme nets $200,000 in Texas.** Word on the street is that ATM skimming is now the most profitable crime, say Houston, Texas police who arrested two men accused of putting a skimming device on a local bank's ATM. A Houston police lieutenant says that the suspects were caught putting the device on an ATM in a bank on Montrose Boulevard, near the University of St. Thomas on January 19. This incident is another example of increased ATM-related crimes. Security experts have predicted that ATM fraud will increase in 2010. The lieutenant, who works in the police department's financial crimes division, says the police watched as the suspects sat across the street in a black Cadillac Escalade, monitoring the ATM through binoculars. Once they saw customers pull up, the suspects moved in closer and turned on their wireless camera. The camera let them see the customers as they entered their banking PIN into the ATM's keypad. One Houston area bank reports it lost more than $200,000 because of the skimming device, police say. "We have had suspects tell us that the word among criminals on the street is that skimming is a much more profitable crime to commit, not only because the amount of money they are able to steal very quickly, but also because it is less likely that they will be detected," the lieutenant explained.
Source: http://www.bankinfosecurity.com/articles.php?art_id=2115

[Return to top]

Transportation Sector

24. *January 28, Wall Street Journal* – (International) **FAA seeks checks of pilot oxygen systems on Boeing jets.** U.S. aviation regulators have ordered inspections of emergency cockpit oxygen systems on roughly 1,300 Boeing jetliners operated by U.S. carriers, more than a decade after the manufacturer first warned airlines that certain parts posed potential fire hazards. Covering three separate Boeing models, from domestic workhorse 737 aircraft to the longest-range international 747 jumbo jets, rules proposed by the Federal Aviation Administration call for checks of some cockpit oxygen hoses that can catch fire if there is a short circuit in a nearby electrical panel. The proposed inspections and fixes, released at the end of last week, are expected to be embraced by foreign regulators. Starting more than a decade ago, Boeing received reports of problems caused by current flowing through part of the stowage box for pilot oxygen masks, which eventually can result in a hose melting or burning. The initial incident was reported on a Boeing 757 in 1997. In response, the company in 1999 issued its first round safety bulletins covering 757s and three other aircraft models, according to a Boeing spokeswoman. Boeing urged inspections of low-pressure oxygen hoses and, if necessary, replacing them with new parts that wouldn't conduct electricity. The work was to be completed "at the earliest opportunity when manpower, material and facilities are available." Complying with manufacturer bulletins is voluntary. The issue of hazardous hoses moved back into the spotlight in June 2008, when an Airborne Express Boeing 767 cargo plane caught fire while preparing to push back from a gate at San Francisco International Airport. The fire burned a hole through the top of fuselage before it was extinguished, but the crew escaped without injury. On Friday, the FAA issued separate but identical proposed safety directives for 737s, 747s and 767s. It had previously issued essentially the same proposals covering more than 480 Boeing 757s in September 2009.
Source:
http://online.wsj.com/article/SB10001424052748703906204575028171518328544.html?mod=WSJ_hpp_MIDDLENexttoWhatsNewsTop

25. *January 27, Associated Press* – (California) **Planes get too close on approach to LAX.** Federal Aviation Administration officials say an error by an air traffic controller allowed a commuter plane to get too close to a Boeing 767 on approach to Los Angeles International Airport last week. An FAA spokesman said Tuesday that an American Eagle Embraer E135 came within three miles of the tail of the Chilean-based LAN Airlines plane on January 19 while flying at about 7,000 feet. Pilots are required to maintain five miles of separation to avoid wake turbulence that can send smaller planes out of control. A controllers union spokesman told San Diego's KGTV that controllers are overworked and understaffed. The spokesman called the error "serious" but said it was not caused by understaffing and there was no imminent danger to the smaller plane.
Source: http://abcnews.go.com/Business/wireStory?id=9671861

26. *January 27, Wall Street Journal* – (National) **FAA cites progress in drive to improve commuter airline safety.** Federal aviation regulators said new government and industry initiatives have succeeded in lifting the overall safety of U.S. commuter airlines. In a report released Tuesday, the Federal Aviation Administration said the

improvements stem in part from closer government oversight of pilot training and from moves by carriers to better identify and track weak pilots. The report follows a wide-ranging FAA effort to plug numerous safety gaps exposed by the February 2009 crash of a Colgan Air turboprop near Buffalo, N.Y., which killed 50 people. The high-profile crash sparked public and congressional criticism of widespread problems at many commuter airlines, such as inadequate pilot training, low salaries and lack of cockpit discipline. Commuter carriers, which account for roughly half of all U.S. commercial flights, contract to carry passengers on behalf of mainline carriers on routes that are not served by larger jets. The report gives generally high grades to most airlines, along with FAA inspectors and managers in responding to the agency's call last June to step up commuter safety. The safety improvements range from more-focused government surveillance of pilot training to better tracking of new pilots' performance. The report also lays out progress FAA officials believe the industry has made in collecting and analyzing data from airline incidents and mishaps. The FAA's campaign to improve safety focused on the qualifications, training and flight-time limits of commuter crews. Many commuter pilots were hired on with minimal levels of experience at the controls. The campaign also sought to encourage larger airlines to share safety data and "best practices" with their commuter partners. One problem the FAA was particularly concerned about was an apparent lack of cockpit discipline among some commuter pilots. The crew of the Colgan plane that crashed last year, for example, failed to properly follow checklists and engaged in idle chatter just moments before the crash. The report says the FAA will continue to prod pilot unions to develop new guidelines to "clearly articulate the aviation community's expectations for professional behavior" on flight decks.
Source:
http://online.wsj.com/article/SB10001424052748703410004575028423631473944.html?mod=googlenews_wsj

[Return to top]

Postal and Shipping Sector

27. *January 27, News 10 Now* – (New York) **White powder mailed to Bishop Ludden High School.** When the Bishop Ludden school's principal in Geddes, New York opened a standard white envelope addressed to the school Monday morning, he never expected he would have to call the authorities. "Our principal received a letter in the mail that upon opening it, contained a suspicious white substance," said the superintendent of schools for the Diocese of Syracuse. "At that time, he immediately called upon his assistant principal. They kicked the emergency plan into place. They called the Geddes police and involved the police immediately." A Geddes police investigator says the letter was handwritten. But what it said can not be revealed at this time. The powder it was covered in, unknown. The superintendent says the principal was the only one that came into contact with the envelope and that students were never in danger. "The ventilation in this particular part of the building was off. Our buildings are all steam heat so there is no ventilation running in the wintertime. There's no forced air. So that's why we knew that students were not in danger," he said. Geddes Police

are working with postal inspectors and the FBI. They say they do not want to reveal too many details at this time as to avoid the likes of a copy cat.
Source: http://news10now.com/watertown-north-news-1052-content/top_stories/494252/suspicious-powder-sent-to-bishop-ludden-hs

[Return to top]

Agriculture and Food Sector

28. *January 27, Associated Press* – (National) **Survey: Honeybee colony collapse losses declining.** Fewer beekeepers are reporting evidence of a mysterious ailment that had been decimating the U.S. honeybee population. But losses due to colony collapse disorder remain high enough to keep beekeepers on edge, and longtime stresses on bees such as starvation and poor weather add to the burden. A survey of beekeepers for the January issue of the Journal of Apicultural Research found that the percentage of operations reporting having lost colonies but without dead bees in the hives — a symptom of colony collapse disorder, or CCD — decreased to 26 percent last winter, compared to 38 percent the previous season and 36 percent the season before that. Also, the percentage of colonies that died that displayed the CCD symptom was 36 percent last winter, down from 60 percent three winters ago, the survey found. The earliest reports of CCD date to 2004, and scientists still are trying to find a cause.
Source: http://www.nytimes.com/aponline/2010/01/27/us/AP-US-Farm-Scene-Disappearing-Bees.html?_r=2

29. *January 26, CBS News* – (National) **Lab confirms Salmonella strain in outbreak.** A strain of Salmonella has been linked to an outbreak that made 189 people sick in 49 states Monday during testing at the University of Iowa. Thirty-five people have been hospitalized from the strain since July, but no deaths have been reported. The Centers for Disease Control and Prevention, the Food and Drug Administration and the Department of Agriculture's Food Safety and Inspection Service are investigating the outbreak. According to the University of Iowa, on Saturday, Daniele International recalled more than 1.2 million pounds of its ready-to-eat sausage products because of a possible salmonella contamination. The Iowa Department of Public Health investigated a case of salmonella poisoning in the state and found leftover sausage in the patient's home and sent the meat to the University of Iowa's Hygienic Laboratory for testing. Using DNA fingerprinting, the lab confirmed the sausage matched the same strain as the national outbreak.
Source: http://www.cbsnews.com/stories/2010/01/26/health/main6144342.shtml

30. *January 26, Bloomberg* – (International) **Kraft, GM shut Venezuela plants to dodge blackouts.** Kraft Foods Inc. and a Coca-Cola Co. bottler are among international companies in Venezuela that will close plants for one day a week to escape rolling blackouts amid the worst power crisis in six years. The companies and other users are trying to cut electricity use by 20 percent while escaping the blackouts that hurt output and damaged equipment in the manufacturing center of Valencia, the head of the energy commission at the Industrial Chamber of Commerce of Carabobo state said. The

chamber Monday agreed with Corpoelec, the state power company, to cease operations for one day a week in return for an end to the rolling blackouts of as much as five hours a day. Companies had lengthened their hours to make up for the blackouts, eliminating the energy savings, the head of the energy commission said Tuesday. Coca Cola Femsa SAB, which bottles Coca Cola drinks, Chrysler Group LLC and Motors Liquidation Co., which control the country's biggest carmaker, General Motors Venezuela, and Owens- Illinois Inc., the world's largest maker of glass containers, are among the 200 companies that will close plants, said the president of the chamber of commerce. The president of Ford Motor Co.'s local unit said his company would not be affected by the weekly closures because it produces 80 percent of its own power. He had said Ford was one of the companies to be included in the agreement. "We're making process adjustments to keep from being affected," he said. The company was able to keep producing through two-hour unscheduled blackouts last week, and is preparing for the possibility of more frequent outages, he said. Kraft, maker of mayonnaise, Oreo cookies and Velveeta processed cheese, has "been able to adapt to the current schedule (one day off per week) such that there has been no impact on production," a company spokesman said.
Source: http://www.businessweek.com/news/2010-01-26/kraft-coca-cola-ford-shut-venezuela-plants-to-escape-blackout.html

[Return to top]

Water Sector

31. *January 27, Associated Press* – (Tennessee) **Chattanooga sewage leak into Tennessee River fixed after 137 million gallons released.** Chattanooga officials fixed a wastewater plant power failure that released 137 million gallons of sewage and stormwater into the Tennessee River. A city spokesman said workers restored the Moccasin Bend treatment plant to full capacity about 4:30 a.m. Wednesday and stopped the overflows caused by the Tuesday morning power outage that shut down the plant's pumping system. He said the 137 million gallons of untreated sewage and storm water waste released into the river represents less than 1 percent of the total flow released from TVA's Chickamauga Dam. An estimated 80 billion gallons of water flowed through the dam Tuesday. He said an overflow area under the Market Street Bridge was sanitized Wednesday morning.
Source: http://www.whnt.com/news/sns-ap-tn--river-sewage,0,6227072.story

32. *January 27, Roanoke Times* – (Virginia) **Pulaski County's water plant shut down.** Schools distributed bottled water to students and officials encouraged households and businesses to conserve Tuesday after flooding at Claytor Lake shut down Pulaski County's water treatment plant in Virginia. Officials warned residents outside the town of Pulaski that the public water supply could run out while the plant was offline. Late Tuesday, the Pulaski County Public Service Authority issued a boil order for any home that had lost service or water pressure on Tuesday. "Low pressure or dewatered lines and tanks may allow contaminated water to enter the distribution system," the notice said. The recommendation is to boil water through Thursday as a

precaution. The first outages were reported late Tuesday afternoon in Dublin and Draper. Sediment and debris from widespread flooding caused most of the problems, the assistant county administrator said. Some of the raw water coming into the plant in Draper was "almost mud. If we try to run it, it could damage the equipment," he said. About 4,500 business and residential customers across the county could be affected by the shutdown. Under normal conditions, the plant treats and distributes about 2 million gallons of water per day, he said. Town of Pulaski residents have a separate water source and were not affected. Most Snowville residents rely on well water. Public Service Authority employees were working to get the system back up and hoping water conditions in the lake will improve soon, he said. County officials ordered bottled water to be delivered Tuesday and expected to soon set up distribution sites for residential customers in need of drinking water, he said. Residents were asked to delay activities that would use a large volume of water, such as doing laundry and washing cars.
Source: http://www.roanoke.com/news/nrv/wb/234421

33. *January 27, Wheeling News-Register* – (West Virginia) **Rising water calls attention to broken gauge at plant.** A broken gauge at the Wheeling Water Treatment Plant has made it harder for local officials to get an accurate reading of the level of the Ohio River. The gauge was reported as broken earlier this week by the National Weather Service (NWS) after officials began focusing on rising water levels in the Ohio Valley. "Those gauges are owned by the U.S. Geological Survey, so we were not really sure what the problem was," a representative for the NWS said. He said that forecasters noticed the gauge was stuck at around 15 feet, about half of the actual river level. The gauge was also reported broken to the Ohio County Emergency Management director who said that he was not sure when the USGS would be able to fix it. Though the gauge had been reported as broken, a lead hydrolic technician for the West Virginia Water Science Center said he was not aware of the problem. He did say he would be contacting a technician and that the issue would be taken care of soon. He said a number of things could cause the gauge to fail, including blockages such as logs and other debris or low temperatures freezing the gauge. In the meantime, local officials have had to measure the water manually. As of Tuesday afternoon, the river was predicted to crest around 35.5 feet, just under the 36-foot flood stage for the area and a full foot off of the 36.6 feet needed to flood Wheeling Island, according to the National Weather Service.
Source: http://www.news-register.net/page/content.detail/id/533696.html?nav=510

34. *January 26, Greenwood Commonwealth* – (Mississippi) **Collapsed manhole puts crews to test.** A collapsed manhole bordering the Yazoo River in North Greenwood, Mississippi, has had city crews scrambling. "They've been working on it since last night," the mayor said. The mayor said the elevated manhole, which is near Claiborne Avenue and Virginia Street, is part of the city's sanitary sewer line. On January 26, river water was rushing into the open sewer line. She said for now, the collapse poses no threat to residents in North Greenwood. The director of the Department of Public Works said the situation will require the construction of a temporary dam so that crews can stop the flow of river water and determine the extent of the sewer line problem. Such a dam will have to be built by a private contractor since the city does not have the

equipment necessary to undertake that kind of specialized work. There are other considerations that must be taken into account prior to attempting repairs, such as locating and avoiding all underground cables and pipelines that might be in the vicinity of the sewer line, he said. Herring said he had no exact idea as to the diameter of the sewer line in question but that the line connects to Pumping Station No. 1.
Source:
http://gwcommonwealth.com/articles/2010/01/26/news/top_stories/01262010news05.txt

35. *January 26, KNSD 7 San Diego* – (California) **Pump station blamed for flooding from storms.** A pumping station in Mission Beach, California, may have been the reason for much of the flooding during last week's storms. On Monday, San Diego City Council members issued a request for emergency repairs on the pump station located on Santa Clara Place in Mission Beach. Many houses and businesses were damaged because of the station's inablilty to pump enough water during last week's storms. "I want staff to provide an immediate solution for this rain in terms of trying to increase the pumping capacity here — and from a long term perspective what the city needs to do to redesign this so it works," the council president pro tem said. A time frame for repairs has not yet been determined. A long term solution to increase the pumping capacity is still being worked on by the city.
Source: http://www.nbcsandiego.com/news/local-beat/Pump-Station-Blamed-For-Flooding-From-Storms-82661552.html

36. *January 26, Rapid City Journal* – (North Dakota; South Dakota) **Thousands without water after storm.** The chairman of the Cheyenne River Sioux Tribe, declared a state of emergency on the sprawling reservation Tuesday. Damage from recent ice storms and strong winds left the reservation without power and water. The Tri-County/Mni Waste Water System at Eagle Butte is operated by the Cheyenne River Sioux Tribe. The system supplies water to approximately 14,000 people on the Cheyenne Indian Reservation, the communities of Faith, Isabel and Dupree, and rural portions of Dewey, Ziebach, and Meade counties. Tri-County's water treatment plant lost power one week ago when power lines started falling after days of fog and icing, according to the manager. With approximately four million gallons of water held in storage reservoirs, the system had enough capacity to continue operating for a few days. On January 22, generators were moved to the water system's alternate pumping site on the Cheyenne River. It was not feasible to take generators 20 miles to the new pumping station on the Oahe Reservoir. As the power failures spread, a generator was used to operate the water treatment plant 20 miles south of Eagle Butte, but the plant was not operating at capacity. Without water to fill storage reservoirs, the system's users gradually started drawing down those reserves. On Sunday night, generator and filter problems at the treatment plant caused about 800,000 gallons of water to flood the treatment plant. The water was discovered Monday morning. Employees spent Monday pumping water out of the plant and assessing the damage. On Tuesday several electric motors were in Pierre being rebuilt. The damage to the plant's computerized equipment was also being assessed. If the plant is operational by Friday, only the town of Eagle Butte will have water service. The manager is reluctant to predict when system will be fully

operational.
Source: http://www.rapidcityjournal.com/news/article_95604146-0ab5-11df-88a7-001cc4c03286.html

37. *January 25, U.S. Environmental Protection Agency* – (Guam) **EPA penalizes Guam Waterworks Authority additional $57,000 for failing to complete water tank assessment.** The U.S. Environmental Protection Agency today penalized the Guam Waterworks Authority (GWA) $57,000 for failing to fully comply with a stipulated order to make improvements to its drinking water and wastewater systems. GWA was penalized for the continued failure to meet a December 31, 2008 deadline for completing a condition assessment to determine the structural stability and soundness of steel tank water reservoirs that need immediate assessment, and for failure to complete a condition assessment of the remaining steel tank water reservoirs by December 31, 2009. Some of the tanks have severely corroded exterior walls, roofs, or valves, or are missing tank parts.
Source: http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/f4148f0ea72c588e852576b70002cfd2!OpenDocument

[Return to top]

Public Health and Healthcare Sector

38. *January 26, Kansas City Star* – (National) **U.S. gets 'F' in preparation for threat of biological terrorism, report concludes.** The United States has failed to adequately prepare for the threat of biological terrorism, a report concluded Tuesday. The Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism gave the government an "F" for bioweapon preparedness. It said the blame could be shared among Democratic and Republican administrations and Congress. The White House does not agree with the commission's failing grade, an unnamed source told the Associated Press. A report issued Monday by Harvard University said al-Qaida was still pursuing biological, chemical, and nuclear weaponry. The commission said this country's response to the H1N1 flu showed that authorities were not ready for a bioterror attack. Preventing a bioterror attack is difficult, so the best deterrent is a strong response mechanism, the report said. The commission did find progress in some of the 17 areas studied. It gave the government above-average grades for openness of public communications regarding weapons of mass destruction, and for the President's efforts to prevent the spread of nuclear weapons. But it gave a "D+" to the government's efforts to regulate "high containment" laboratories that study dangerous pathogens.
Source: http://www.kansascity.com/news/politics/story/1710371.html

39. *January 26, My Web Times* – (Illinois) **Phone threat locks down Ottawa Regional Hospital.** A threatening telephone call to Ottawa Regional Hospital from a 42-year-old man allegedly distraught over a teddy bear gift locked down the medical facility for an undisclosed period Monday night. According to police reports the Ottawa man

identified himself to a staff nurse, who supposedly recognized his voice from previous contacts, and threatened to "shoot up the place." Police were then notified of the phone threat at 8:35 p.m. A lockdown of the building was immediately organized by an off-duty Ottawa police employee working as a night security officer in accordance with standard procedure at the medical facility. Ottawa police, assisted by La Salle County Sheriff's officers, rushed to the caller's home northwest of the city where they found the man "distraught, angry and disoriented." Allegedly, the man said he was upset about a stuffed teddy bear of his that was given by a relative to another relative who was a patient at the hospital. Authorities said the man had ingested an unknown quantity of prescription medications earlier in the day and, because of his agitated condition, had to be transported by Ottawa emergency personnel to the very hospital he had just threatened. A spokesperson for the La Salle County State's Attorney's Office said the incident is under review and charges against the man may be filed in the near future. A spokeswoman with Ottawa Regional Hospital declined to comment.
Source: http://mywebtimes.com/archives/ottawa/display.php?id=396427

40. *January 26, Homeland Security Today* – (National) **Hospital surge capacity for mass casualties still a problem.** The Government Accountability Office (GAO) on Monday issued an updated report, "State Efforts to Plan for Medical Surge Could Benefit from Shared Guidance for Allocating Scarce Medical Resources," that says many hospitals in the United States are unprepared for treating the overwhelming "surge" of victims from a large scale mass casualty event. GAO said that "based on a review of state emergency preparedness documents and interviews with 20 state emergency preparedness officials...many states had made efforts related to three of the four key components of medical surge that GAO had identified — increasing hospital capacity, identifying alternate care sites, and registering medical volunteers, but fewer had implemented the fourth: planning for altering established standards of care. More than half of the 50 states had met or were close to meeting the criteria for the five medical-surge-related sentinel indicators for hospital capacity reported in the Hospital Preparedness Program's 2006 midyear progress reports. In a 20-state review, GAO found the following. All 20 were developing bed reporting systems and most were coordinating with military and veterans hospitals to expand hospital capacity. Eighteen were selecting various facilities for alternate care sites. Fifteen had begun electronic registering of medical volunteers, and fewer of the states — 7 of the 20 — were planning for altered standards of medical care to be used in response to a mass casualty event." State officials in GAO's 20-state review "reported that they faced challenges relating to all four key components in preparing for medical surge," GAO stated.
Source: http://www.hstoday.us/content/view/11933/149/

41. *January 26, CNN* – (International) **FDA recalls more than 2 million needles used in port implants.** Millions of needles used in ports implanted under the skin of chronically ill patients are being voluntarily recalled, the U.S. Food and Drug Administration (FDA) announced Tuesday. More than 2 million Huber needles, manufactured by Nipro Medical Corp. in Japan and distributed by Exelint International Corp., headquartered in Los Angeles, California, are affected. Huber needles are used primarily in hospitals and clinics — and in some instances by patients receiving long-

term treatment at home — to draw blood or to inject medicine, other nutritional solutions or blood products. They are used with ports, which are small medical appliances placed under the skin. The Class 1 recall — denoting that the FDA considers the product to be of the highest risk — involves Exel/Exelint Huber needles, Exel/Exelint Huber Infusion Sets and Exel/Exelint "Securetouch+" Safety Huber Infusion Sets. Approximately 6 million Huber needles are used each year in the United States. The agency determined that 60 to 70 percent of Exelint's needles "cored," or cut slivers of silicone, when inserted into ports, raising the possibility of the silicone slivers entering the veins, damaging the port itself or harming the surrounding tissue. There have been reports of leakage, the FDA said, but none of silicone entering the vascular system as a result of the needles. It said anyone using the products should stop immediately and return any unused needles to Exelint. Investigations are being done of needles from 20 companies, and 10 of those investigations have been completed, the agency said. So far, no other products have been recalled. The FDA said it has sent letters to all Huber manufacturers asking them to address any design or manufacturing problems. There was no immediate public comment from Exelint.
Source: http://www.cnn.com/2010/HEALTH/01/26/needles.recall/?hpt=T2

[Return to top]

Government Facilities Sector

42. *January 27, Associated Press* – (Louisiana) **4 men accused of phone plot make court appearance.** Three of four men charged with infiltrating the New Orleans office of a Democratic U.S. Senator returned to court today for private appointments in the pretrial services department. Three of the suspects carried suitcases and declined comment. Federal authorities said 2 of the men posed as telephone workers wearing hard hats, tool belts and fluorescent vests when they walked into the senator's office inside a federal building in New Orleans on Monday. The other two are accused of helping to organize the plan. The most well-known of the suspects is a 25-year-old whose hidden-camera expose posing as a pimp with his prostitute infuriated the liberal group ACORN.
Source: http://www.wdam.com/Global/story.asp?S=11887630

43. *January 26, The Register* – (International) **Defects in e-passports allow real-time tracking.** Computer scientists in Britain have uncovered weaknesses in electronic passports issued by the US, UK, and some 50 other countries that allow attackers to trace the movements of individuals as they enter or exit buildings. The so-called traceability attack is the only exploit of an e-passport that allows attackers to remotely track a given credential in real time without first knowing the cryptographic keys that protect it, the scientists from University of Birmingham said. What's more, RFID, or radio-frequency identification, data in the passports cannot be turned off, making the threat persistent unless the holder shields the government-mandated identity document in a special pouch. "A traceability attack does not lead to the compromise of all data on the tag, but it does pose a very real threat to the privacy of anyone that carries such a device," the authors wrote. "Assuming that the target carried their passport on them, an

attacker could place a device in a doorway that would detect when the target entered or left a building." To exploit the weakness, attackers would need to observe the targeted passport as it interacted with an authorized RFID reader at a border crossing or other official location. They could then build a special device that detects the credential each time it comes into range. The scientists estimated the device could have a reach of about 20 inches. "This would make it easy to eavesdrop on the required message from someone as they used their passport at, for instance, a customs post," the authors wrote.
Source: http://www.theregister.co.uk/2010/01/26/epassport_rfid_weakness/

For another story, see item **27**

[Return to top]

Emergency Services Sector

44. *January 27, Associated Press* – (Florida) **Florida teens escape juvenile program in stolen fire truck.** Two teens fled from a juvenile diversion program at a Florida Keys campground in a stolen firetruck. The teens have been arrested and charged with grand theft auto. The truck belonged to the chief of the Big Pine Key Fire Department. Authorities say a Camp Sawyer counselor called the Monroe County sheriff's office Monday morning to report that the teens were missing from the site on West Summerland Key. Deputies then learned of the missing fire truck. The boys were caught 90 miles away. A Sheriff's Office spokeswoman says she can remember of police cars being stolen, but this is the first case of a stolen firetruck.
Source: http://www.foxnews.com/story/0,2933,584051,00.html

45. *January 26, WXIX 19 Cincinnati* – (Ohio) **Cincinnati police officers beginning to wear miniature cameras.** Cincinnati Police officers are now field testing wearable clip-on video cameras. The device is called AXON. It is described as an on-officer tactical computer and an audio-video recorder that captures incidents from the officer's perspective. The AXON (which stands for Autonomous eXtended on-Officer Network) is a small, lightweight headset that fits into an officer's ear and aims wherever he or she looks. Besides recording up to 10.5 hours of video, it can serve as an earpiece for police radios. "This is an additional piece of evidence that the officers can use throughout the course of his or her duties," said a spokesman for Taser Inc. The camera is designed to enable full audio-video recording from a head camera the size and weight of a standard Bluetooth headset and transfer it securely to a computer hard drive without interference. "It helps me to remember an incident under stress where I might not remember what I did or what I said and it will be right there for everybody to view including myself," said a Cincinnati police officer. The individual systems costs about $1500.
Source: http://www.fox19.com/global/story.asp?s=11879054

46. *January 25, Terre Haute Tribune-Star* – (Indiana) **Power outage knocks out Vigo 911 central dispatch for about an hour.** A power outage in Terre Haute, Indiana shut down electrical service at Vigo County central dispatch for approximately an hour

Monday night. At least one power transformer apparently exploded Monday evening, cutting power to the Sheriff's Department, where central dispatch is housed, the sheriff said. A backup generator kicked on and powered most of the lights and other equipment at the jail, "but it did not repower 911," he said. There is also a backup battery system, "but, for some reason, it failed to kick on," he said. Despite the outage, 911 calls were handled by Indiana State University police, the sheriff said. "Our rollover system worked," he assured. Regular power was restored to 911 about 9:20 p.m. The timing of the power outage was especially unfortunate since ice and snow had made roads potentially hazardous in the Terre Haute area Monday night. Several property damage accidents were being reported, he said.
Source: http://www.tribstar.com/news/local_story_025215855.html

[Return to top]

Information Technology Sector

47. *January 27, V3.co.uk* – (International) **TechCrunch hacked twice in 24 hours.** Security experts are warning webmasters to be on their guard, after popular technology blog TechCrunch was hacked for the second time in 24 hours. Users were greeted this time with a four-letter tirade against the site's founder. The first hack happened at around 6am GMT on January 26, when visitors saw a blank page with a brief message and a link to a site containing links to "adult and pirated material", according to a Sophos senior technology consultant. Later that morning the site posted a brief story about the hack. "At this point we are still gathering information on how the site was compromised, and will update this post with additional information," it said. However, the consultant said in a blog post that the site was compromised again within 24 hours, and that the hackers left another message. "So [name of TechCrunch founder], how much did all the media coverage yesterday brought you in trough the welcome.html ad you forced people to? What a [expletive] retarded move was that you [expletive]. You should be thanking me and [expletive] on my [expletive] for not deleting everyone on the box and publishing the mysql, if that's what you want O.K, I can do that," the message read. According to the consultant, the message also included a link to a web site "hosting links to hardcore file-sharing torrents". TechCrunch has yet to elaborate on how the hackers managed to deface its site.
Source: http://www.v3.co.uk/v3/news/2256848/techcrunch-hacked-again

48. *January 27, IDG News Service* – (International) **PlayStation 3 hack released online.** Days after announcing he had managed to hack Sony's PlayStation 3 console to run his own software, the hardware hacker has released the exploit online. The hacker, who is best known for cracking Apple's iPhone, said in a blog posting that he had decided to release the exploit to see what others could do with it and because he wanted to move on to other work. With the release of the exploit online many programmers will likely start to examine the PlayStation 3 for ways to get deeper into the system. For some the prime goal will be to crack the encryption system that ensures illegally copied games cannot be played on the console while others will likely be motivated by the technical challenge of running their own software on the powerful PlayStation 3

platform. The exploit the hacker has found works with the PlayStation 3's OtherOS feature that allows a second operating system to be installed on the machine. This feature was discontinued on newer model machines, the so-called "PS3 Slim" consoles. Sony is also examining the code. Its Tokyo-based gaming unit, Sony Computer Entertainment, said it is looking into the claims made by the hacker and declined to comment until it has finished its investigation.
Source:
http://www.computerworld.com/s/article/9149398/PlayStation_3_hack_released_online

49. *January 27, SC Magazine* – (International) **The popularity of Apple devices is attracting malware, according to a report from Intego.** Amid speculation that Apple is set to introduce its tablet device on January 28 at a press event in California, a discussion of the security implications will not likely be mentioned. While the device is already being touted as a game-changer in the publishing industry, reportedly introducing a new digital platform with a ten-inch screen for the delivery of newspaper and magazine content, what is likely to follow within months of the debut, if history is any precedent, is a new wave of malware targeting the device. Users tuning in for their daily news feed or perusing copies of their favourite magazines may become victims of new iterations of malware likely intended to steal their passwords and personal information to then be offered for sale in the nether regions of cyberspace. This scenario echoes Apple's January 2009 introduction of new software at Macworld Expo, a forum the company traditionally uses to roll-out new products and to announce updates to existing ones. According to an annual report, The Year in Mac Security from Intego, following the release of an update to Apple's iWork 2009 suite of software, malware writers immediately introduced the iServices Trojan Horse as a supplement hidden inside an installer available to users downloading bootlegged versions from BitTorrent and other grey and black market distributors of pirated software. The Intego report stated that following up on the successful implementation, the same cyber gang issued the next version of their malware planted in Adobe Photoshop CS4 for Mac, again distributed via BitTorrent. In April, Intego detected proof-of-concept malware, Tored.A, that was created in RealBasic code. This self-contained application tried to copy itself to root folders on Macs and then siphoned email addresses from the Mac utility address book and sent emails containing the malware. The virus was also capable of linking the user machine to a botnet and recording keystrokes.
Source: http://www.scmagazineuk.com/the-popularity-of-apple-devices-is-attracting-malware-according-to-a-report-from-intego/article/162463/

50. *January 27, The Register* – (International) **Google Toolbar caught tracking users when 'disabled'.** Google has updated its browser toolbar after the application was caught tracking urls even when specifically "disabled" by the user. In a January 25 blog post, a Harvard professor and noted Google critic provided video evidence of the Google toolbar transmitting data back to the Mountain View Chocolate Factory after he chose to disable the application in the browser window he was currently using. The Google toolbar offers two disable options: one is meant to disable the toolbar "permanently," and the other is meant to disable the app "only for this window." In a statement passed to The Register, Google has acknowledged the bug. According to the

statement, the bug affects Google Toolbar versions 6.3.911.1819 through 6.4.1311.42 for Internet Explorer. An update that fixes the bug is now available here, and the company intends to automatically update users' toolbars sometime today. The statement also says that the bug does not occur if you open a new tab after disabling the toolbar for a particular window. In the statement, Google goes on to say that the bug disappears if you restart your browser, but this does not quite make sense. If you are interested in disabling Google toolbar for a particular window, you are not going to close that window.
Source:
http://www.theregister.co.uk/2010/01/27/google_toolbar_caught_transmitting_data_when_disabled/

51. *January 26, Help Net Security* – (International) **Cybercrime increasing faster than company defenses.** Cybercrime threats posed to targeted organizations are increasing faster than many organizations can combat them. Moreover, a new survey suggests the threat of cybercrime is heightened by current security models that are only minimally effective against cyber criminals. More than 500 respondents, including business and government executives, professionals and consultants, participated in the survey. The survey is a cooperative effort of CSO, the U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte's Center for Security & Privacy Solutions. The 2010 CyberSecurity Watch Survey uncovered a drop in victims of cybercrimes (60 percent vs. 66 percent in 2007), however, the affected organizations have experienced significantly more attacks than in previous years. Between August 2008 and July 2009 more than one third (37 percent) of respondents experienced an increase in cybercrimes compared to the previous year. Although the number of incidents rose, the ramifications have not been as severe. Since 2007, when the last cybercrime survey was conducted, the average monetary value of losses resulting from cybercrimes declined by 10 percent. This can likely be attributed to an increase in both IT security spending (42 percent) and corporate/physical security spending (86 percent) over the past two years.
Source: http://www.net-security.org/secworld.php?id=8769

52. *January 26, Help Net Security* – (International) **Devious ransom trojan takes data hostage.** Taking data hostage is not a new invention in the world of cybercrime but a trojan currently infecting computers does it in a way that can leave the victim unaware that he has been scammed. The CRO at F-Secure, says, "When the W32/DatCrypt trojan infects a computer, it makes it seem as if some files, such as Microsoft Office documents, video, music and image files have been "corrupted", when the files have in fact been encrypted by DatCrypt. Next the trojan creates what looks like an authentic message from Windows, advising the user to download and execute the "recommended file repair software" called Data Doctor 2010." If this utility is downloaded and executed, the user receives a message that it can "only repair one file in unregistered version". In order to repair — or more accurately, decrypt — more files, the user has to buy the product for $89.95. After the money is paid, the software does return access to the files.
Source: http://www.net-security.org/malware_news.php?id=1208

53. *January 26, DarkReading* – (International) **New attack uses Internet Explorer's own features against it.** A researcher at Black Hat DC, which runs from January 31 until February 3, will demonstrate how an attacker can steal files from a victim's machine by abusing a combination of actual features in Internet Explorer. A security consultant with Core Security Technologies says popular features in IE, such as URL Security Zones and the browser's file-sharing protocol, can together be abused to execute an attack that results in the attacker being able to read all files on the victim's machine. The consultant plans to release proof-of-concept code for the attack next month after Black Hat DC, and after Microsoft issues a security update for the attack, which affects IE versions 6 and above, he says. The attack requires the user to click on a malicious link. The group manager of Microsoft's Trust The attack basically abuses the way features in IE are designed, the consultant says, and it only works when a combination of features are abused in the attacks. A single feature cannot be abused to wage the attack, he says. It does not, however, allow the attacker to execute code remotely or to control the victim's machine.
Source:
http://www.darkreading.com/vulnerability_management/security/client/showArticle.jhtml?articleID=222500167&subSection=End+user/client+security

54. *January 26, DarkReading* – (International) **Report: More than 560,000 websites infected in Q4.** A total of 5.5 million Web pages on more than 560,000 Websites were infected in the fourth quarter, according to new data, with evidence that attackers are waging less noticeable exploits in order to remain under the radar. Dasient, which compiled the data from its proprietary malware analysis tool that gathers information on malware attacks on Websites, says the fourth-quarter 2009 numbers are actually a slight decline from the third quarter, when it found more than 640,000 infected Websites and 5.8 million infected Web pages. The decline, in part, could have to do with smarter, more sophisticated attacks: Infections of newly compromised Websites of 10 or more pages on average hit about 24 percent of the pages on those sites, a jump of 19 percent from Q3. The infections basically spread to more pages on each site in the fourth quarter, according to Dasient's report. Another indication that attackers are launching stealthier and more efficient attacks is in the number of programs used in the attacks. The average number of programs loaded onto a victim's machine from an infected Website was 2.8, while two years ago attackers would typically send a dozen or more malicious programs onto these machines.
Source:
http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=222500206&subSection=Attacks/breaches

55. *January 26, V3.co.uk* – (International) **Hackers ran detailed reconnaissance on Google employees.** The hackers who infiltrated the computer systems of Google earlier this month first carried out sophisticated reconnaissance and may even have posed as friends of Google employees, according to a McAfee chief technology officer. In a project dubbed Operation Aurora by the security giant, hackers are likely to have used sophisticated social engineering techniques and advanced reconnaissance work to target individuals at the companies who had access to sensitive data. "In this case we saw a

lot more reconnaissance done upfront, which is a shift people may not have been aware of," the technology officer told V3.co.uk. This could involve compromising the social networking accounts of employees' friends, then sending them malicious links which they are more likely to click on because they appear to come from a friend. The technique is not new, but it would be the first time it has been detailed in such a high-profile attack.
Source: http://www.v3.co.uk/v3/news/2256804/hackers-carried-detailed

For another story, see item **13**

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

56. *January 26, FierceTelecom* – (Texas) **Copper theft shuts down AT&T service in Dallas.** AT&T's landline voice customers in Dallas, Texas were without phone service on January 25 when thieves made off with 200 feet of copper cabling. Since the cable theft was done in the very early morning, AT&T said only about 20 customers reported they were without service in the afternoon of January 25, meaning that the outage was not widespread. Stealing these particular copper cables, which AT&T estimates could fetch no more than $2000 on the scrap metal market, came at a major risk because they are high tension and are located right next to utility electric lines. There has been no shortage of copper thieves being electrocuted when they mistakenly cut into an adjacent utility electric wire. After a slight lull, a jump in copper prices has spurred on a new wave of copper theft.
Source: http://www.fiercetelecom.com/story/copper-theft-shuts-down-t-service-dallas/2010-01-26

57. *January 26, Lake County News-Chronicle* – (Minnesota) **Damaged line cuts phone, internet service in parts of Duluth, Lake and Cook counties.** A steam pipe that broke in a manhole in Duluth is believed to be the cause of damage to a fiber-optic line that has cut phone and Internet service to thousands in Northeastern Minnesota. Qwest Communications has determined that the damage occurred in Duluth north of Qwest's downtown location. "A steam pipe burst and the hot steam hit one of our fiber lines and melted it," said a spokeswoman for Qwest. "We now have people there that are working trying to fix it as soon as we can." Damage to the fiber-optic line took place just before 11 a.m. and is affecting phone coverage for Qwest customers in Two Harbors, Grand Marais, Silver Bay, and Finland, she said. As repairs were being made, service also was disrupted in Duluth's Lakeside neighborhood and a few other parts of

town. Frontier Communications, which runs some of its traffic through the Qwest fiber-optic line, reported that about 4,000 of its customers in the same coverage areas also have been affected. Cell phone service is affected along Highway 61 between Two Harbors and Grand Marais, as well. Customers should be able to dial locally but will have trouble making toll or emergency calls, the spokesman said.
Source:
http://www.twoharborsmn.com/event/article/id/158591/group/News/publisher_ID/36/

58. *January 26, Defense Industry Daily* – (National) **U.S. Navy beefs up commercial satellite capacity for ships.** In the early weeks of Operation Iraqi Freedom, the U.S. military satellite communications capacity was overwhelmed by the demand from U.S. troops for satellite bandwidth to transmit voice and data communication. In response, the U.S. military dramatically increased its use of commercial satellite capacity to meet the explosion of demand. A study by the Satellite Industry Association found that 80 percent of all U.S. military satellite communication during the Iraq invasion was carried on commercial satellites. The then-assistant secretary of defense for networks and information integration estimated that the U.S. military purchased between $200 million and $300 million worth of commercial satellite services during the first year of the war. Recognizing the military's reliance on commercial satellites, the US Navy undertook an effort, called the Commercial Broadband Satellite Program (CBSP), to develop and deploy satellite communication terminals specifically designed to increase the Navy's commercial satellite communications capability. The Navy expects to eventually deploy 200 of the high capacity terminals, which will be able to send data at a speedy 21.4 Mbps as opposed to the current Inmarsat and Commercial Wideband Satellite Program terminals, which can only send data at 4 Mbps.
Source: http://www.defenseindustrydaily.com/US-Navy-Beefs-Up-Commercial-Satellite-Capacity-for-Ships-06128/

[Return to top]

Commercial Facilities Sector

59. *January 26, Associated Press* – (Alaska) **Bomb donated to Kodiak museum was a dud, after all.** It now turns out that a World War II relic detonated earlier this month in Kodiak, Alaske was a dud, after all. The 1,263-pound 'Deck-Busting' aerial bomb was donated to the Kodiak Military History Museum, whose director determined it might still contain explosives. An ordnance detail from Fort Richardson in Anchorage traveled to Kodiak and examined the device. They determined the bomb still contained Dunnite, a highly explosive material also known as "Explosive D." However, Army officials now say it was drywall and not Dunnite inside the relic. A spokesman told the Kodiak Daily Mirror that the drywall had been soaked in some type of petroleum product that had turned yellow and made it look suspicious.
Source: http://www.ktuu.com/Global/story.asp?S=11883054

60. *January 26, Fresno Bee* – (California) **Clovis police probe teen link to explosives.** Clovis police are asking residents near Keats and Magnolia avenues to

watch for suspicious activity related to reports of teenagers using homemade explosives. A Clovis police spokeswoman said residents in the area have reported hearing large firecracker-like explosions coming from a nearby park. On Sunday about 6 p.m., police responded to a report of three high school-age boys exploding homemade bombs. When police arrived they found pieces of two plastic bottles that had been exploded, but no suspects. And Tuesday, the Clovis Fire Department discovered three plastic "bottle bomb" devices at the same park. Two of them had exploded, the third was intact but inert. The police spokewoman said bleach may be one of the ingredients used in the devices. She warns that the homemade devices can be just as dangerous as illegal fireworks.
Source: http://www.fresnobee.com/updates/story/1797810.html

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

61. *January 27, Athens Banner-Herald* – (Georgia) **Rains cause dam to burst; no damage reported.** Heavy rains caused a dam on an unnamed creek near the Atlanta Highway-Epps Bridge Parkway interchange to burst recently, but no flooding or damage was reported. Stormwater flooded the pond behind the dam during storms late Sunday or early Monday, overtopping it and eventually causing it to crumble, said a spokesman of the Georgia River Network. Water from the pond flowed harmlessly into a nearby box culvert, said the director of the Athens-Clarke Transportation and Public Works Department. The dam was decades old and probably not built to handle all of the runoff from the now-heavily developed area around the pond, said a rural water resource specialist for the Georgia Soil and Water Conservation Commission. The commission owns hundreds of dams, but not that one, he said. The owner of the dam had been warned several times in recent years that it appeared to be in poor condition, according to the department director said. He said he could not recall who owned the property. The state Environmental Protection Division (EPD) regulates privately owned dams. EPD could require the dam to be rebuilt or simply allow the creek to continue flowing freely, he said. About 2.5 inches of rain came down in Athens on Sunday and Monday, according to the National Weather Service.
Source: http://www.onlineathens.com/stories/012710/new_555184617.shtml

62. *January 27, Lake Wylie Pilot* – (South Carolina) **Dam gate opens as Lake Wylie reaches flood level.** After driving rains caused scattered flooding across the region earlier this week, Duke Energy began releasing more water through the Lake Wylie Dam on Monday to keep the lake below flood levels. Just before noon Tuesday, the lake level measured 3 inches below what is considered full pond, a level that would

cause flooding. A gate was opened 10 feet at the Lake Wylie Dam on Monday to prevent water from spilling over the banks of Lake Wylie. A spokesman for Duke, said Tuesday that Lake Wylie will probably remain at full pond for several days, but that barring more rain, the lake is not expected to flood. "We're trying to keep it right now around full pond," he said. "We would expect it to stay pretty much in that range." However, the company noted on its Web site that people living on creeks and streams in low-lying areas should pay special attention to changing weather conditions. "It's not just the lakes. A lot of times, it's creeks and tributaries that feed the lakes," he said. More severe conditions were found elsewhere. Six Duke-managed lakes, including Wateree, Rhodhiss, and Lookout Shoals, maxed out beyond full pond. Rhodhiss and Lookout Shoals are both located north of Lake Wylie, while Wateree is to the south. Some lakes operated by Duke reached up to 3 feet beyond full pond Tuesday and 4 feet Monday, officials said. Duke tries to keep its lakes at a target range. The target for Lake Wylie is 3 feet below full pond to allow for significant rainfall such as the one Sunday night on the northern reaches of the Catawba River. Creeks swelled throughout the river basin as 2 to 4 inches of rain fell in areas where lake levels already were high, he said.
Source: http://www.heraldonline.com/109/story/1897359.html?storylink=omni_popular

63. *January 25, Agence France Presse* – (International) **Huge 'iceberg' threatens Siberian dam: report.** A Siberian dam where 75 people were killed in a disaster last year is now threatened by a huge "iceberg" that has formed due to its stalled turbines and winter conditions, a Russian daily said Monday. The ice mass, which weighs 25,000 ton and is 22 meters (72 feet) thick in some points, could lead to a new catastrophe at the Sayano-Shushenskaya hydroelectric power plant, two scientists told the Gazeta daily. However the company which operates the plant, state-owned RusHydro, denied there was any risk to the dam straddling the powerful Yenisei River in the Khakassia region of southern Siberia. Gazeta, which ran a photograph of the ice mass along the bottom of the dam, said it had formed because RusHydro was allowing water to flow out of the reservoir via a spillway which had never before been used in winter. The August 17, 2009 accident damaged the turbines through which the water normally passes, forcing the dam operator to use the spillway to ease pressure on the dam. A large cloud of mist thrown up from the spillway has been freezing and turning into ice flakes that fall on the roofs of various structures at the bottom of the dam, building up into a thick mass, Gazeta said. The ice could cause parts of the power plant to collapse said a scientist quoted by the Gazeta. RusHydro said it was monitoring the situation and dismissed the possibility of another disaster at the dam. A Russian government investigation concluded that the August disaster was caused by a technical fault in one of the plant's turbines and blamed senior officials, including some at RusHydro, for failing to prevent the disaster.
Source: http://www.terradaily.com/reports/Huge_iceberg_threatens_Siberian_dam_report_999.html

[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