# Department of Homeland Security Daily Open Source Infrastructure Report for 29 February 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- According to internal government documents obtained by ABC News, thousands of foreign student pilots who do not have the proper visas have been able to enroll in U.S. flight schools and obtain pilot licenses. Under laws passed in the wake of the September 11 attacks, American flight schools are only supposed to provide pilot training to foreign students who have been given a background check by the Transportation Security Administration and have a specific type of visa. (See item **15**)
- The Milwaukee Journal Sentinel reports Milwaukee police are investigating the apparently intentional disruption of Milorganite fertilizer production this week at the Jones Island sewage treatment plant in Wisconsin. Six of 12 sewage sludge dryers used in Milorganite production had to be shut down Tuesday morning after a manually operated valve for a cold water pipe to a dryer had been opened. (See item **32**)



## 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. *February 27, Reuters* – (Texas) **Loss of wind causes Texas power grid emergency.** A drop in wind generation late on Tuesday, coupled with colder weather, triggered an electric emergency that caused the Texas grid operator to cut service to some large industrial customers, the grid agency said on Wednesday. Electric Reliability Council of

Texas went to the second stage of an emergency plan at 6:41 p.m., ERCOT said in a statement. System operators curtailed power to interruptible customers to shave 1,100 megawatts of demand within ten minutes. Interruptible customers are generally large industrial customers who are paid to reduce power use when emergencies occur. No other customers lost power during the emergency, ERCOT said. Interruptible customers were restored in about 90 minutes and the emergency was over in three hours. ERCOT said the grid's frequency dropped suddenly when wind production fell from more than 1,700 megawatts, before the event, to 300 MW when the emergency was declared. ERCOT declares a stage 1 emergency when power reserves fall below 2,300 MW. A stage 2 emergency is called when reserves fall below 1,750 MW. At the time of the emergency, ERCOT demand increased from 31,200 MW to a peak of 35,612 MW, about half the total generating capacity in the region, according to the agency's Web site.
Source:
http://www.reuters.com/article/domesticNews/idUSN2749522920080228?feedType=RSS&feedName=domesticNews&rpc=22&sp=true

2. *February 27, Electric Light & Power/Utility Automation & Engineering T&D News* – (National) **Energy expert raises key proposals.** To meet future power demand and provide quality, reliable electricity to American homes and businesses, policymakers and state regulators need to change the way electric power utilities do business now, the executive director of the Galvin Electricity Initiative said Wednesday during the National Electricity Delivery Forum in Washington, D.C. "Our electric power system has been in a sub-prime mortgage-like era for decades," he said. "There are no technological or economical obstacles to modernizing the U.S. electric grid, only policy and regulatory barriers that must be eliminated. If states open up the electricity market and offer utilities incentives for integrating smart grid technology and giving consumers control of their own energy use, everyone will win. Consumers gain better service and a smaller carbon footprint while utilities gain much-needed upgrades and a system that is less vulnerable to cyber-attack."
Source:
http://uaelp.pennnet.com/display_article/321376/22/ARTCL/none/none/1/Energy-expert-to-regulators-and-utilities:-

3. *February 26, Environment News Service* – (National) **Eroding Alaska native village sues energy companies.** The arctic coastal village of Kivalina and a federally recognized tribe, the Alaska Native village of Kivalina, are suing two dozen oil, coal, and power companies that they claim have made the climate warmer, causing their land and homes to slide into the Chukchi Sea. Nine oil companies, 14 power companies, and one coal company are named in a lawsuit filed Tuesday in U.S. District Court in San Francisco. The original village was located at the north end of the Kivalina Lagoon but was relocated. Due to severe sea wave erosion during storms, Kivalina hopes to relocate again to a new site nearby and studies of alternate sites are ongoing. Financing for the move is estimated to cost hundreds of millions of dollars. The village should stand a good chance of a court upholding a claim that they suffered damages because of global warming, a climate change scientist said.

Source: http://www.ens-newswire.com/ens/feb2008/2008-02-26-094.asp

[Return to top]

## Chemical Industry Sector

4. *February 26, Comtex* – (National) **ACC encouraged by congressional effort to make chemical security regulations permanent.** The House Committee on Homeland Security held a hearing on Tuesday on the "Chemical Anti-Terrorism Act of 2008." ACC supported legislation granting the Department of Homeland Security the authority to issue federal chemical security regulations, and worked closely with Congress and DHS to ensure that effective rules were issued in 2007 covering all of the nation's chemical facilities.
   Source: http://www.foxbusiness.com/article/acc-encouraged-congressional-effort-make-chemical-security-regulations_495981_1.html

[Return to top]

## Nuclear Reactors, Materials, and Waste Sector

5. *February 28, Associated Press* – (National) **Ahead of the bell: nuclear plant security.** Representatives from the companies and agencies involved in last year's high-profile case of Wackenhut security guards caught nodding off at a nuclear power plant will be on Capitol Hill Thursday. Congressional members and officials from the U.S. Nuclear Regulatory Commission (NRC), Exelon Corp., and Wackenhut will examine security and government oversight at a Senate subcommittee hearing scheduled to begin at 10 a.m. After guards at the Peach Bottom plant in Pennsylvania were found to be sleeping on the job, Exelon Corp. said Wackenhut would be out of its ten nuclear plants by July, and an in-house security force would take over. Wackenhut officials have called the guards' behavior an "anomaly." Since the Peach Bottom incident, the NRC has asked commercial nuclear power plant operators for more information about their security.
   Source:
   http://biz.yahoo.com/ap/080228/nuclear_plant_security_ahead_of_the_bell.html?.v=1

6. *February 27, Reuters* – (International) **Shipping bottlenecks may halt nuclear renaissance.** Nuclear power may face supply problems as worries over the safety of radioactive material limit its movement around the globe. The nuclear industry relies on ships to get its uranium fuel, and shipping companies and ports face tight regulations over the handling of radioactive goods. About 20 million packages of all sizes containing radioactive materials are transported around the world annually on public road, railways, and ships, but fewer and fewer transporters want to deal with the burdensome materials. "It will move in increasing volume internationally as demand grows – not only in the fuel cycle sector, but in medical applications as well," said the secretary general of the World Nuclear Transport Institute.
   Source: http://www.guardian.co.uk/feedarticle?id=7341449

7. *February 27, Pahrump Valley Times* – (National) **NEI courts volunteers for interim**

**storage.** With uncertainties swirling around the proposed Nevada radioactive waste site, the nuclear industry has mounted a campaign to court communities that might be willing to host interim storage of its used fuel. Officials with the Nuclear Energy Institute are meeting with governors, state legislators, and other elected leaders, including those in states where nuclear waste has sat for years at decommissioned power plants, said an NEI executive. Talks are moving forward with two or three communities, and more sites are expected to show interest. He said some communities were among the 11 sites that at one time volunteered to host a nuclear waste reprocessing plant for the government. Those were in New Mexico, Washington, Idaho, Illinois, Tennessee, Kentucky, Ohio, and South Carolina. Energy Department leaders have discouraged talk of interim nuclear waste storage, where potential hosts are expected run into a gantlet of legal, technical, and political challenges like those that confronted the consortium that tried to establish a storage site on the Goshute Indian reservation in Utah. The director of the Office of Civilian Radioactive Waste Management has testified to Congress that by the time a temporary storage site is located, licensed, built, and opened for business, Yucca Mountain would be close to finished anyway.
Source: http://www.pahrumpvalleytimes.com/2008/Feb-27-Wed-2008/news/19960495.html

[Return to top]

## Defense Industrial Base Sector

8. *February 27, Navy Times* – (National) **C4ISR problems could delay cutter construction.** The Coast Guard may endure more delays in completing its inaugural national security cutter, the Bertholf, because of shielding and security problems with the ship's command and communications suite, according to an announcement posted Monday on a Coast Guard Web site. Inspections by the Coast Guard, contractors, and the Navy's Space and Naval Warfare Systems Command have "identified discrepancies that will be added to the list of [information assurance] remediation actions that need to be completed prior to final onboard testing," the announcement said. The news was the first time the Coast Guard appeared to confirm rumors that the C4ISR systems aboard the Bertholf did not comply with federal and Department of Defense information-security standards, known as TEMPEST. Whether or not there are delays, the ship – scheduled for delivery in spring –will be in "special commission status" when it enters the fleet, so that it can operate the systems it needs to get from the yard in Pascagoula, Mississippi, to its new homeport in Alameda, California. Until it satisfies the TEMPEST and information assurance requirements, the cutter cannot take on any Coast Guard missions.
Source:
http://www.navytimes.com/news/2008/02/coastguard_bertholf_delays_080226w/

9. *February 27, CNN* – (National) **$40 billion Air Force tanker deal expected.** The U.S. Air Force is expected to announce this week a $40 billion contract to replace its aging fleet of air refueling tankers. The contract would start to replace the almost 500 planes in the tanker fleet with 149 new planes, and options could extend the contract up to $100 billion, Pentagon officials said. Since 2001, the Air Force has been trying to replace the

tanker fleet, which has some planes close to 50 years old, according to Air Force statistics. The average age of the fleet is more than 24 years, according to Air Force officials, while the average age of a U.S. commercial airline fleet is about nine years.
Source: http://www.cnn.com/2008/US/02/27/airforce.tankerdeal/index.html

[Return to top]

## Banking and Finance Sector

10. *February 28, Daily Progress* – (National) **Security code easy hacking for UVa student.** A University of Virginia graduate student and two fellow hackers say they have cracked the encryption code that protects billions of credit cards, subway passes and security badges. With readily available equipment that cost less than $1,000, the student and his two Germany-based partners dismantled a tiny chip that is found inside many "smartcards" and mapped out its secret security algorithm. With the cryptographic formula in hand, the hackers were then able to run it through a computer program that tried out every possible key. It broke the encryption after a few hours. If they were to try again, he said, it would take a matter of minutes. "I don't want to help attackers, but I want to inform people about the vulnerabilities of these cards," said the Ph.D. candidate in computer engineering at UVa who is originally from Germany. The wireless chips -- which employ technology known as radio-frequency identification, or RFID -- are found inside most modern credit cards, car keys, security keycards and subway passes. The chips send an encoded numeric signal to the reading device, which allows the user to simply wave their card to gain access to secure buildings, remotely unlock a car, pay for public transportation and much more. The three computer whizzes announced their findings at the Chaos Communications Congress in Berlin, an annual worldwide convention of hackers. They are not releasing the details of how they beat the chip's security code. But, the student added, if they could defeat the code, it is possible that criminals might also have done so.
Source: http://www.dailyprogress.com/servlet/Satellite?pagename=CDP/MGArticle/CDP_BasicArticle&c=MGArticle&cid=1173354778618

11. *February 28, Rocky Mountain News* – (Colorado) **State issues warning on latest e-mail scam.** On Wednesday, Colorado's attorney general warned consumers and businesses about a new e-mail scam related to messages claiming to be from the U.S. Department of Justice. The e-mails concern a supposed consumer complaint filed against the recipient and usually contain an attachment. The attachment is either a blank complaint form or some other document. The official advises consumers not to open the attachment because it might contain a computer virus or other malicious software. The Justice Department does not send messages to the public via e-mail. Similar hoaxes have recently been conducted in the names of other government entities, the Justice Department said in a statement. Consumers who have received such bogus e-mails are asked to file a complaint at ic3.gov., which is the federal government's Internet crime complaint center.
Source: http://www.rockymountainnews.com/news/2008/feb/28/state-issues-warning-on-latest-e-mail-scam/

12. *February 28, CNN* – (National) **What bad banking news means to you.** In the past year there have been four bank failures. And the chairman of the Federal Deposit Insurance Corp (FDIC) and banking industry experts foresee many bank failures down the road. "Regulators are bracing for 100-200 bank failures over the next 12-24 months," says an analyst with the financial services firm, the Stanford Group. Expected loan losses, the deteriorating housing market and the credit squeeze are blamed for the drop in bank profits. The problem areas will be concentrated in the Rust Belt, in places like Ohio and Michigan and other states like California, Florida and Georgia. The number of institutions categorized as "problem" institutions by the FDIC has also grown from 50 at the end of 2006 to 76 at the end of last year. The FDIC insures deposits in banks and thrift institutions. The federal agency was created during the Great Depression in response to thousands of bank failures. Experts say people should not panic.
Source: http://www.cnn.com/2008/LIVING/personal/02/27/bank.safety/index.html

13. *February 27, Dallas Morning News* – (Texas) **Dallas FBI warns about Nigerian scam using its letterhead.** The Nigerian scammers are using a new tactic to trick folks out of their money: the Federal Bureau of Investigation or at least the FBI's official-looking letterhead, featuring the Dallas bureau's address in downtown Dallas. The real FBI warned Internet surfers Wednesday to be on the watch for slick-looking letters and e-mails with FBI letterhead. The latest scam mentions a purported gentleman at Dallas/Fort Worth International Airport who needs someone with no terrorist or criminal background to help transfer $10 million. All he needs is a bank account records to help with the transfer. The letter is signed by a special agent in charge. "While most law-abiding citizens will recognize these letters as obvious forgeries, it is important to note that millions of dollars in losses are suffered by victims of these schemes each year," the real FBI said in its statement Wednesday.
Source:
http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/022808dnbusnigerianscam.1b00a43.html

14. *February 27, New York Times* – (National) **Ranking corporate America on identity theft.** Based on consumer complaints to the Federal Trade Commission, a senior fellow at the Berkeley Center for Law and Technology at the University of California at Berkeley compiled a preliminary report dubbed "Measuring Identity Theft at Top Banks," which purports to rank the overall vulnerability of the world's largest financial institutions, phone companies and retailers -- and their customers -- to identity theft. None of these corporations disclose internal data on the number of account takeovers or fraudulent accounts created. The researcher thinks that instead of swallowing the claims in commercials about identity-theft protection, consumers should be able to "vote with their feet" and pick the most secure stores, phone companies and financial institutions. The country's largest banks and phone companies showed up most frequently. So, to account for size in the financial services industry in particular, the researcher factored in the total amount of deposits per bank as of December 31, 2006. He also concedes there are limitations to the study. "It needs more information to be useful to consumers," he

said. “But it should be useful for banks, who themselves are probably curious what their competitors’ fraud rates are.”
Source: http://bits.blogs.nytimes.com/2008/02/27/ranking-corporate-america-on-identity-theft/?ref=technology

[Return to top]

## Transportation Sector

15. *February 27, ABC News* – (National) **9/11 redux: ‘Thousands of Aliens’ in U.S. flight schools illegally.** Thousands of foreign student pilots have been able to enroll and obtain pilot licenses from U.S. flight schools, despite tough laws passed in the wake of the 9/ll attacks, according to internal government documents obtained by ABC News. “Thousands of aliens, some of whom may very well pose a threat to this country, are taking flight lessons, being granted FAA certifications and are flying planes,” wrote a Transportation Security Administration official in 2005, complaining that the students did not have the proper visas. Under the new laws, American flight schools are only supposed to provide pilot training to foreign students who have been given a background check by the TSA and have a specific type of visa. But in thousands of cases that has not happened, according to the documents and current and former government officials involved in the program. The official says in one year alone, 2005, he found that some 8,000 foreign students in the FAA database had gotten their pilot licenses without ever being approved by the TSA. The FAA and Homeland Security are now starting to crack down on a number of flight schools suspected of training students illegally.
Source: http://abcnews.go.com/Blotter/story?id=4353991&page=1

16. *February 27, Associated Press* – (National) **New way to test nuclear detectors urged.** The government needs to develop a better way to evaluate the effectiveness of technology to detect nuclear and radiological material at U.S. ports, according to a report commissioned by the Homeland Security Department. Congress and its investigative arm, the Government Accountability Office, have been skeptical about the department’s testing of such systems. As a result, the department called for an independent audit into its testing. The department plans to spend about $350 million to develop and deploy next generation radiation monitors that will screen cargo, cars and trucks that come through ports, according to a homeland security official. The most the department can spend on this program is $1.2 billion, but current tests show that these systems can be deployed for far less, the official said. The goal is to purchase about 800 of these next generation monitors called Advanced Spectroscopic Portals, over the course of the next five years. The monitors are expected to cost about $360,000. Lawmakers have questioned whether the new technology offers much improvement over current monitors. But the department’s testing has found that the next generation monitors, produce much fewer false positives. The 800 monitors will not replace all the existing systems. In some ports, the first generation models will remain in place.
Source: http://news.yahoo.com/s/ap/20080228/ap_on_go_ca_st_pe/nuclear_detectors_1

[Return to top]

## Postal and Shipping Sector

Nothing to report.

[Return to top]

## Agriculture and Food Sector

17. *February 27, Reuters* – (National) **Meat companies race to save consumers time.** Consumers can now select from an array of meat that has been cooked, breaded, marinated, and packaged in various ways so that they can prepare it quickly without the hassle of thawing, cutting, or seasoning. While chicken has led the way in this meat-case evolution, beef and pork are now getting into the act. Many more changes are in the pipeline, according to meat industry experts. In an era of tough competition and greater health-consciousness, meat companies are spending more than ever before on product development, said an agricultural economist at Kansas State University. Tyson Foods Inc., the world's largest meat company, hopes to accelerate that trend with its "Discovery Center." The $45 million center is part research lab, part test kitchen, and gathers 120 research and development employees in its 100,000 square feet of space. The center has a U.S. Agriculture Department-inspected meat plant, which allows the company to know exactly how a new product will flow from plant to a store or restaurant under real-world conditions, said a director at the center.
Source: http://news.yahoo.com/s/nm/20080227/us_nm/meat_innovation_dc;_ylt=Avn98vjpmRXNsZ7W2XmJWZkWIr0F

18. *February 27, Reuters* – (National) **Congress asks companies to do more on food safety.** U.S. food suppliers are overhauling their own food safety rules, executives from companies involved in recent food recalls said on Tuesday, but lawmakers said the industry must do more to prevent future outbreaks. A series of high-profile food safety scares in the past two years have aggravated concerns among consumers, Congress, and federal health regulators. Food executives told a House Energy and Commerce subcommittee they are implementing a series of initiatives to improve food safety at their facilities. Lawmakers told industry officials that while foodmakers have apologized, they have not done enough to prevent future recalls and unsafe products from reaching consumers. Among the measures recently proposed by Congress is combining the 15 government agencies that handle food safety under one roof, and giving the Food and Drug Administration and the U.S. Agriculture Department the ability to conduct a mandatory recall.
Source: http://news.yahoo.com/s/nm/20080227/hl_nm/food_safety_dc_1

[Return to top]

## Water Sector

19. *February 27, San Francisco Chronicle* – (California) **Rain brings sewage into San Francisco Bay.** There have been more large, environmentally damaging sewage spills in

the San Francisco Bay Area in the first two months of 2008 than in the last seven and a half months of last year, a San Francisco Chronicle analysis has found. The spills continued over the weekend when two in Marin County dumped thousands of gallons of sewage into San Francisco Bay and an adjoining waterway. About 8,000 gallons of sewage spewed out of a blocked pipe in the Marin County community of Sleepy Hollow on Sunday. Workers with the Ross Valley Sanitation District managed to contain some of the sewage, but a lot of it poured into Corte Madera Creek, according to the U.S. Environmental Protection Agency. That same day, 6,000 gallons of raw sewage overflowed in San Rafael. The administrator of the San Rafael Sanitation District said a giant wad of paper towels blocked a pipe, forcing sewage and runoff water out of a manhole cover where it flowed across the street and into the San Rafael Canal, which flows into San Pablo Bay. Experts believe the large amount of rain so far this winter is at least partly responsible for the number of sewage spills. The regional clean water compliance chief for the U.S. Environment Protection Agency said the main problem is that there are thousands of miles of sewer pipes in the Bay Area and San Francisco, some of which are a hundred years old and made out of brick or clay. Some of the joints are fastened together with tarred rope, according to water district officials. Many of the pipes are cracked and have roots growing into them, allowing rainwater to flow in and mix with the sewage, overwhelming the systems during winter storms.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/02/27/BA6UV906K.DTL

20. *February 28, WGCL 46 Atlanta* – (Alabama, Florida, Georgia) **Water-sharing deal unlikely.** A water-sharing agreement among Georgia, Alabama, and Florida appears to be unlikely. The parties have scheduled no more negotiations between now and the deadline on Saturday. A spokesman for Alabama's governor said Wednesday that confidential talks appear all but dead. Representatives from the three states met on Monday. The states' differences are the subject of lawsuits in federal courts in Alabama and Florida, so continued litigation could determine how the water is divided. Hopes for an out-of-court agreement began to fade Tuesday when Georgia's governor accused his counterparts of lacking resolve in the negotiations. He told the Associated Press the two other states' problems are not as critical as Georgia's.
Source: http://www.cbs46.com/news/15434933/detail.html

[Return to top]

## Public Health and Healthcare Sector

21. *February 28, Associated Press* – (National) **CDC panel urges flu shots for all children.** All children -- not just those under 5 -- should get vaccinated against the flu, a federal advisory panel said Wednesday. The panel voted to expand annual flu shots to virtually all children except infants younger than 6 months and those with serious egg allergies. That means about 30 million more children could be getting vaccinated. If heeded, it would be one of the largest expansions in flu vaccination coverage in U.S. history. The Advisory Committee on Immunization Practices said all children should start getting vaccinated as soon as possible, acknowledging that many doctors have already ordered their vaccine for the 2008-2009 season and may not be able to give the shots until 2009-2010. The panel's advice is routinely adopted by the Centers for

Disease Control and Prevention, which issues vaccination guidelines to doctors and hospitals. The panel said that should be expanded to include children up to age 18. Children who stay home sick from school cause parents to stay home, so reducing the illness in this group should cut down days of lost work, some experts said. Before the vote, the panel heard a presentation of a study that found the vaccine was 75 percent effective in preventing hospitalizations from the flu in children 6 months to 23 months.
Source: http://www.foxnews.com/story/0,2933,333408,00.html

22. *February 28, Associated Press* – (International) **WHO confirms urban yellow fever threat in Paraguay.** The World Health Organization said Wednesday it has confirmed the first cases of yellow fever in an urban area of Latin America in six decades. A yellow fever chief for the U.N. health agency said the mosquito-born disease can spread particularly fast in suburbs and cities and warned that vaccinations are needed to stem the outbreak. WHO officials said there have been nine confirmed cases in the suburbs of Paraguay's capital, Asuncion. The agency said three people had died, though Paraguayan authorities put the death toll at eight. WHO experts said a mass vaccination campaign was under way in Paraguay and was closely monitoring vaccine supplies. The yellow fever outbreak is Paraguay's first since 1974. The last yellow fever cases in any Latin American city were in the 1940s in Brazil.
Source: http://www.cnn.com/2008/WORLD/americas/02/28/yellow.fever.ap/index.html

23. *February 27, HealthDay News* – (International) **Some countries may have slowed bird flu's spread.** Several strains of H5N1 bird flu virus that afflicted southern China were blocked from entering neighboring Thailand and Vietnam, say University of California, Irvine, researchers who conducted the first-ever statistical analysis of H5N1's genetic diversity. The information gleaned from this analysis may help scientists better understand how the strain migrates and, in future, determine the success of programs to halt the spread of the virus. The study was published online February 27 in the journal *PLoS One*. The type of genetic analysis used in this study could help health officials in different countries determine whether their efforts to control H5N1 are effective, the UCI researchers said.
Source: http://health.usnews.com/usnews/health/healthday/080227/some-countries-may-have-slowed-bird-flus-spread.htm

24. *February 27, Network World* – (National) **Are healthcare organizations under cyberattack?** Healthcare organizations feel under increasing attack from the Internet, while security incidents involving insiders and disappearing laptops with sensitive data are piling up. On top of that, there is now the prospect of a surprise audit from the federal government agency in charge of overseeing the HIPAA security and privacy rules. "Healthcare organizations store a lot of valuable personal, identifiable information such as Social Security numbers, names, addresses, age, in addition to banking and credit-card information," says a researcher at Atlanta-based security services firm SecureWorks. SecureWorks has recorded an 85 percent increase in the number of attempted attacks directed toward its healthcare clientele by Internet hackers, with these attempts jumping from 11,146 per healthcare client per day in the first half of 2007 to an average of 20,630 per day in the last half of last year through January of this year.

SecureWorks believes that some of the most sought-after information is from patients who are members of preferred medical network plans, which hackers turn around and sell as credentials to criminals specializing in illegal immigration. Insider attacks, too, are also a worry. Lost and stolen laptops have also been a problem, with disclosure of missing personal information related to patients or employees. The U.S. Department of Health and Human Services, which oversees Health Insurance Portability and Accountability Act compliance, has contracted with the firm PricewaterhouseCoopers to conduct surprise audits of hospitals this year, says a Gartner analyst.
Source: http://www.pcworld.com/article/id,142926-c,techindustrytrends/article.html

## Government Facilities Sector

25. *February 28, WCVB 5 Boston* – (Massachusetts) **Security tight at college after threats made.** In Massachusetts, Bridgewater State College was holding classes Thursday, although attendance was expected to be low after death threats were made at the campus. The College president was named in the latest death threats found in a women's bathroom. There have been a series of at least seven written death threats discovered at the campus recently. One said, "Death 2/28," and another said, "Murder, 2/28." Other threats were found earlier in the week, all mentioning the date of February 28. Campus officials have brought in extra campus police for Thursday's classes. But some students said they will probably stay away from classes anyway. Bridgewater State was not the only Massachusetts college beefing up security Thursday. Police presence on the University of Massachusetts Amherst campus was also increased after a janitor found a threatening message, and a building at Framingham State College was evacuated Wednesday after a student found a note mentioning a bomb. There is no evidence that any of the threats were connected.
Source: http://www.thebostonchannel.com/news/15434573/detail.html

26. *February 27, Associated Press* – (North Carolina) **Mock gunman drill terrifies students, faculty at North Carolina University.** Elizabeth City State University (ECSU) is offering counseling to faculty and students after some became unknowing participants in an emergency response drill. An armed man burst into a classroom Friday, threatening to kill students. The drill came eight days after a gunman killed five people and himself in a classroom at Northern Illinois University. The vice chancellor of student affairs said ECSU was testing its response to such shootings. E-mail and text messages were sent five days before the drill, notifying students, staff, and faculty, he said. But not everyone got the word, including the assistant professor, whose American foreign policy class was held hostage. At 1:31 p.m. Friday, e-mail and text messages were sent, saying: "This is a test. ECSU is holding a test drill where an armed intruder will enter a room in Moore Hall and be detained by campus police." After about ten minutes, campus police ended the drill by subduing the man.
Source: http://www.foxnews.com/story/0,2933,333069,00.html

[Return to top]

## Emergency Services Sector

27. *February 28, Desastres.org* – (International) **IAFC seeks best practices in US Critical Infrastructure Protection.** The International Association of Fire Chiefs (IAFC), in coordination with its public-safety partners on the Emergency Services Sector Coordinating Council and the U.S. Department of Homeland Security, is seeking model practices in emergency services critical infrastructure protection and resilience efforts. Infrastructure protection for the emergency service sector comprises the protection of human, physical, and cyber elements that maintain and improve the ability of the sector to protect and preserve its own integrity in an imminent or ongoing emergency. Submissions received by March 3, 2008, will be reviewed by a panel of peers for possible inclusion in a set of model procedures that will be associated with the National Infrastructure Protection Plan, Emergency Services Sector-Specific Plan. The goal of this project is to provide models that will help local and regional entities develop effective and comprehensive emergency plans that include how best to protect the protectors.
Source: http://www.desastres.org/noticias.php?id=28022008-39

28. *February 27, ars technica* – (National) **Senate OKs "enhanced" 911 VoIP requirements.** All VoIP customers are one step closer to having "real" 911 services accessible to them, thanks to the Senate. The body passed the IP-Enabled Voice Communications and Public Safety Act Tuesday. The legislation was approved by the Senate Commerce Committee last year, and will now go on to the House of Representatives for further consideration. The bill will require all VoIP companies to provide enhanced 911 (E911) services to all subscribers. "Enhanced" means that subscribers who dial 911 will be connected to a local operator and their details (phone number, address, etc.) will be transmitted automatically. The bill would give the FCC the authority it needs in order to add 911 requirements into all new phone services as they evolve, without needing Congress' involvement. It also mandates a study to "identify mechanisms and timetables for developing next generation 911 capability ubiquitously," and to identify any technical needs in providing altitude information (helpful for those in high-rises).
Source: http://arstechnica.com/news.ars/post/20080227-senate-oks-enhanced-911-voip-requirements.html

[Return to top]

## Information Technology

29. *February 27, InfoWorld* – (National) **eBay Red Team confab aims to help security officers.** eBay is trying to help CISOs (chief information security officers) build a common front in the war against cybercrime. The company played host to chief security officers and a handful of technology vendors this week, holding its annual Red Team security conference at the company's San Jose, California, campus, billing it as a networking opportunity for security professionals where they could discuss areas of common concern. "What we were trying to do was to get all the CISOs together," said

eBay's CISO. "We're dealing with similar problems, almost all of us." While companies using Internet technology may be facing a common set of problems, they have not always shared information with their peers. That is because if news of a hacked server or a data breach is leaked to the press, it can become a public-relations disaster for the company involved. At this week's conference, CISOs discussed common issues, including how they are pursuing cross-border investigations and what they think of the security products they were using. The second-ever Red Team conference ran Monday and Tuesday. The first day of the conference focused on CISO issues, while on day two, the discussion was opened up to security vendors such as iSight Partners and Cisco, which gave presentations on the state of security.
Source: http://news.yahoo.com/s/infoworld/20080227/tc_infoworld/95624_1

30. *February 27, Computerworld* – (International) **Finjan finds illegal database with more than 8,700 stolen FTP credentials.** A fresh discovery by security vendor Finjan provides yet another example of how easy it is becoming for almost anyone to find the tools needed to break into, infect, or steal data from corporate Web sites. The vendor announced Wednesday that it has uncovered an illegal database containing more than 8,700 stolen FTP server credentials including user name, password, and server addresses. Anyone can purchase those credentials and use them to launch malicious attacks against the compromised systems. The stolen credentials belong to companies from around the world and include more than 2,500 North American companies, some of whose Web sites are among the world's top 100 domains, according to Finjan's CTO. The FTP credentials would allow someone with malicious intent to break into and upload malware to a compromised server with a click or two, he said. "You could pick any server you wanted in the list, pay for it," and launch an attack with very little effort. A trading interface on the server hosting the illegal database allows purchasers to buy FTP server credentials based on the country in which the servers are located, or even by the Google ranking of the Web sites, he said. It also appears designed to give criminals looking to resell FTP credentials a better basis for pricing the stolen data, he said.
Source: http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/08/02/27/Finjan-finds-illegal-database-with-stolen-FTP-credentials_1.html

**Internet Alert Dashboard**

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

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

[Return to top]

## Communications Sector

31. *February 28, CNET News* – (International) **In Pakistan vs. YouTube, it's not all about technology.** The flap earlier this week in which Pakistan Telecom knocked YouTube.com off the Internet for two hours was unusual. It was not like when a court in

Turkey blocked access to YouTube from within the country, or when China restricts Western news sites. Those were country-specific and intentional. The outage on Sunday was global and, as far as we know, unintentional. So what is to stop another Internet service provider -- especially a government-owned one -- from intentionally trying this trick? The short answer is that while the Internet is anarchic, it is not that anarchic. In fact, the way network providers handle Internet routing is very specific and carefully defined in a series of standards. Network providers -- called autonomous systems, or Ass -- are assigned unique ID numbers that are compiled by the Internet Corporation for Assigned Names and Numbers. While ICANN holds the master list of AS numbers, they are actually assigned by allocating large blocks of 1,000 or so at a time to regional address registries. And when one network provider misbehaves and broadcasts a false claim to be the proper destination for certain Internet addresses -- as Pakistan Telecom (AS 17557) did this week -- it is easy enough to figure out what is going on. The Internet may be run by computers, but it is managed by people who share tips and alert each other to potential network problems. Some of these discussions take place on public mailing lists; some occur in more private settings. Many of these network operators know each other personally through groups like NANOG, AfNOG, and SANOG. Human intervention, manual overrides, and personal relationships based on in-person meetings are not perfect: ideally, false broadcasts could be prevented completely through encryption-outfitted mechanisms like Secure BGP. But these less-formal relationships have worked remarkably well, and are (for now at least) the first line of defense against someone learning the lessons from Pakistan Telecom and attempting to do far more damage than merely taking out YouTube for a few hours.
Source: http://www.news.com/8301-13578_3-9880244-38.html?part=rss&subj=news&tag=2547-1_3-0-5

[Return to top]

## Commercial Facilities Sector

32. *February 27, Milwaukee Journal Sentinel* – (Wisconsin) **Sabotage suspected in disruption at Milorganite plant.** Milwaukee police are investigating the apparently intentional disruption of Milorganite fertilizer production this week at the Jones Island sewage treatment plant in Wisconsin. Six of 12 sewage sludge dryers used in Milorganite production had to be shut down Tuesday morning after the incident, said a contract compliance officer with the Milwaukee Metropolitan Sewerage District. Those dryers remained out of service Wednesday. The incident occurred just four days before a new contractor is to take over operations of MMSD's facilities. Around 8:43 a.m. Tuesday, monitors showed temperatures plummeting inside a dryer on the south side of the sludge drying and dewatering facility, said the official. United Water employees subsequently found that the manually operated valve for a cold water pipe to that dryer had been opened. The pipe serves a water-spraying system that is only to be used to quickly reduce temperatures inside the bus-sized dryer in case of an emergency, such as an uncontrolled flame. "This was not an equipment failure," he said. "The valve was opened intentionally." The official declined to describe Tuesday's incident as vandalism, and he declined to discuss whether it was connected to the upcoming change of contractors.

Source: http://www.jsonline.com/story/index.aspx?id=722940

[Return to top]

## National Monuments & Icons Sector

Nothing to Report.

[Return to top]

## Dams Sector

Nothing to Report.

[Return to top]

### DHS Daily Open Source Infrastructure Report Contact Information

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

### DHS Daily Open Source Infrastructure Report Contact Information

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

### Contact DHS

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

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

### Department of Homeland Security Disclaimer