



Department of Homeland Security Daily Open Source Infrastructure Report for 20 February 2007

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- InformationWeek reports the Delaware U.S. attorney on Thursday, February 15, revealed a massive insider data breach at chemicals company DuPont where a former scientist late last year pleaded guilty to trying to steal \$400 million worth of company trade secrets. (See item [13](#))
- The Associated Press reports airlines are investigating why windshields on at least 13 planes cracked at Denver International Airport as winds of up to 100 mph whipped through the foothills in Colorado. (See item [17](#))
- Governor Ed Rendell has ordered an investigation to find out what happened with PennDOT, the Pennsylvania Emergency Management Agency, and other agencies that resulted in hundreds of motorists being stranded in their cars for as much as 24 hours on Interstate 78. (See item [18](#))
- The Chicago Tribune reports hundreds of cattle from Canada, which this month confirmed its ninth case of mad cow disease, have entered the U.S. without government–required health papers or identification tags. (See item [25](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

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 20, Bay City News (CA)* — Chevron releases report on refinery fire.** Hazardous materials released as a result of the January 15 fire at the Chevron refinery in Richmond, CA, remained well under the so-called "reportable release threshold" and did not pose any significant health risk to residents in nearby neighborhoods, Chevron reported last week. The refinery was required to publish a 30-day report on the fire, but is continuing to conduct a "root cause analysis" to determine how and why the fire started and what measures will be taken to prevent any similar incidents from happening in the future. The test results released in the 30-day report confirmed what the refinery and the Contra Costa County Hazardous Materials Program have already reported. The material that caught fire was a known as wash oil, which is very similar to diesel fuel and was being used to clean heavier crude oil residue from inside processing equipment, according to the report. Employees had been shutting down one of the refinery's crude oil units for scheduled maintenance when wash oil from a failed pipe erupted into flames. A total of five alarms were called and a shelter-in-place warning was issued for nearby communities.
Source: http://cbs5.com/local/local_story_050104400.html
- 2. *February 18, MarketWatch* — No timeline for restarting Valero McKee refinery.** Valero Energy Corp. on Sunday, February 18, made tangible progress toward repairing and recommissioning its McKee refinery in Sunray, TX, but the area will remain "highly sensitive" for at least three more days, and returning units to normal may be a lengthy process. The fire that began burning Friday in the refinery's propane deasphalting unit was finally extinguished by Sunday morning, and some essential workers were allowed to return to the plant. Due to the limited access to the facility, the severity of the fire and work required to recommission the plant, restart is unlikely to commence before midweek, Valero spokesperson Rose Brown said. Valero's decision Friday to shut the refinery stemmed in part from the fire's proximity to propane tanks that created the risk of an explosion that a union official said could have potentially leveled the facility. Four spherical propane tanks sit adjacent to the unit which caught fire, a propane deasphalter, said John Alexander, a health and safety specialist with the United Steelworkers. The heat and flames from the fire could have resulted in one of the tanks exploding, he said. Such a blast would likely have caused a chain reaction, he added.
Source: <http://www.marketwatch.com/news/story/no-timeline-restarting-valero-mckee/story.aspx?guid=%7B446BBB12-E8C9-426A-98D2-82BACF2067B4%7D>
- 3. *February 18, Associated Press* — Part of Suncor refinery shut down.** A Sunday morning, February 18, power failure at the 90,000-barrel-a-day Suncor Energy Inc. oil refinery in the Denver suburb of Commerce City, CO, knocked part of the facility out of commission and slashed production capacity, the company reported Sunday. The Canadian company said power was interrupted at the facility about 9 a.m. Sunday and forced a complete shutdown of the site's west plant. The west plant processes sour crude, which contains more impurities than sweet crude. The east side of the facility remained operational. The company said there were no injuries or damage to the plant. The Colorado Department of Health and Environment was notified of the disruption, and Suncor is investigating the cause of the power interruption. The company's Website says the refinery supplies about 35 percent of Colorado's gasoline and diesel fuel and is a major supplier of jet fuel at Denver International Airport and the largest

supplier of paving-grade asphalt in the state.

Source: <http://www.forbes.com/feeds/ap/2007/02/18/ap3440825.html>

4. *February 16, Associated Press* — **Swedish nuclear officials call for IAEA inspections of atomic plants.** Sweden's top nuclear officials on Friday, February 16, decided U.N. experts should be invited to inspect the country's atomic power plants after a string of malfunctions raised concerns about safety. The relatively minor incidents have not posed any threat of radioactive leaks. But the frequency of the problems have sparked calls for a review of the safety controls at the power plants, which generate about half of Sweden's electricity. Friday's announcement came as a water leak forced the shutdown of one of four reactors at Sweden's largest nuclear power plant. Officials from Sweden's nuclear watchdog and managers of the country's nuclear power plants met Friday to call on the government to invite experts from the International Atomic Energy Agency (IAEA) to inspect the country's 10 reactors.

Source: <http://www.signonsandiego.com/news/world/20070216-0652-sweden-nuclearreactor.html>

5. *February 15, Federal Energy Regulatory Commission* — **Commission authorizes two new LNG import terminals; expands natural gas energy infrastructure.** The Federal Energy Regulatory Commission (FERC) approved two new liquefied natural gas (LNG) terminals that could supply approximately 3.1 billion cubic feet (Bcf) of natural gas per day to meet ever increasing demand. After a thorough environmental, security and safety analysis conducted by staff in cooperation with the U.S. Coast Guard and other federal, state and local agencies, the Commission granted authorization to two new onshore LNG terminals that would be located in Jackson County, MS. The projects, which will be located adjacent to one another, are Bayou Casotte Energy LLC and Gulf LNG Energy LLC / Gulf LNG Pipeline LLC. Also, the Commission authorized the expansion of an additional 18.1 miles of 42-inch pipeline in Cameron Parish, LA, that will connect with another recently approved project proposed by Cheniere Sabine Pass Pipeline LP.

Source: <http://www.ferc.gov/press-room/press-releases/2007/2007-1/02-15-07-C-1.asp>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

6. *February 19, WFMY News 2 (NC)* — **Explosion, fire shuts down Winston-Salem plant.** Investigators are still looking for the cause of an explosion that rocked northeast Winston-Salem, NC, on Monday, February 19. Officials at the Oracle Packaging plant on Cunningham Avenue say just after 9:00 am there was an explosion in the building, which then caused a fire. About 60 first-shift employees were evacuated from the building. Oracle Sales and Marketing Director Chris Payne says there were no injuries of any kind reported. Roads leading to the plant were blocked off while emergency crews continue the cleanup and investigation. Oracle makes aluminum foil used in healthcare pharmaceutical, food and tobacco products. Company officials say they're not sure when manufacturing will resume at the damaged plant.

Source: <http://www.wfmynews2.com/news/mostpopular/article.aspx?storyid=80000&provider=top>

7. *February 16, TriCities.com (TN)* — **Sewage, chemical spill at Weyerhaeuser plant.** Emergency crews in Kingsport, TN, worked throughout the night to contain a sewage and chemical spill. Crews said a sewage line backed up at the Weyerhaeuser plant, and some of it overflowed into Reedy Creek. Crews say some of the plant's black liquor, a liquid used to break down tree pulp for paper, also seeped into the creek. Crews tell us there is no danger to the city's water supply. The EPA has been notified of the spill.
Source: <http://www.tricity.com/tristate/tri/news.apx.-content-articles-TRI-2007-02-16-0017.html>

[[Return to top](#)]

Defense Industrial Base Sector

8. *February 16, Associated Press* — **Auditors: Billions squandered in Iraq.** About \$10 billion has been squandered by the U.S. government on Iraq reconstruction aid because of contractor overcharges and unsupported expenses, and federal investigators warned Thursday, February 15, that significantly more taxpayer money is at risk. The three top auditors overseeing work in Iraq told a House committee their review of \$57 billion in Iraq contracts found that Defense and State department officials condoned or allowed repeated work delays, bloated expenses and payments for shoddy work or work never done.
Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/02/15/AR2007021500625.html>
9. *February 15, Government Executive* — **Army National Guard outlines \$24 billion equipment wish list.** The Army National Guard has sent a \$24 billion budgetary wish list to Capitol Hill, detailing thousands of vehicles, radios and other gear it needs over the next six years to fully outfit its units with updated equipment. The "equipment modernization shortfall list" details 25 types of equipment ranging from helicopters to night-vision devices that did not make the cut for the Pentagon's six-year budget projections. National Guard leaders, who have said repeatedly their stateside equipment stocks have been substantially reduced due to operations overseas, said they would need to buy nearly 50,000 new Humvees and trucks, upgrade 159 CH-47 Chinook helicopters and purchase communications and other gear to re-equip their force. To simply get all of its units to C-1 baseline readiness standards — meaning they have 90 percent of their needed equipment on hand to respond to homeland missions and overseas contingencies — the Army Guard still would need \$13.1 billion by fiscal 2013, according to another National Guard Bureau document.
Source: http://www.govexec.com/story_page.cfm?articleid=36141&dcn=to_daysnews

[[Return to top](#)]

Banking and Finance Sector

10. *February 18, Websense Security Labs* — **Multiple organization data security breaches.** Websense Security Labs has received reports of multiple data security breaches. 1) Department of Education, Des Moines, IA: Personal information leaked from an unprotected file located on the department's Website. The file contained nearly 160,000 records of individuals who

obtained a General Educational Development certificate from Iowa between 1965 and 2002. 2) City College of San Francisco, San Francisco, CA: Private information of 11,000 past and possibly current students at City College of San Francisco, leaked from a file posted to the Internet for several years. Due to an incorrect business process, students' details were posted online, allowing a contractor to prepare transcripts. 3) Metropolitan Police Department, Washington, DC: Personal information of nearly 2,000 members of the Metropolitan Police Department has been accidentally released to two Advisory Neighborhood Commission officials who requested information about police overtime. 4) Department of Administrative Services, Hartford, CT: Personal of 1,753 state employees leaked after it was posted to the Department of Administrative Services, Hartford, CT, Website. The personal information was included in a spreadsheet of vendors used by the state that was accessible to the public on the state Website. Officials believe the information was on the website since October 2003. Source: <http://www.websense.com/securitylabs/alerts/>

11. *February 16, Department of Treasury* — **Treasury targets Iranian companies for supporting WMD proliferation.** The Department of Treasury on Friday, February 16, designated three Iranian companies supporting Iran's proliferation of weapons of mass destruction (WMD), Kalaye Electric Company, Kavoshyar Company, and Pioneer Energy Industries Company. This action was taken pursuant to Executive Order 13382, which is aimed at exposing and financially isolating proliferators of WMD and their supporters. The entities designated today are either owned or controlled by the Atomic Energy Organization of Iran (AEOI) or acting for or on its behalf. President George W. Bush designated the AEOI in the Annex to Executive Order 13382, effective June 29, 2005. The AEOI manages Iran's overall nuclear program and reports directly to the Iranian President. Source: <http://www.treasury.gov/press/releases/hp267.htm>

12. *February 16, InformationWeek* — **International thieves arrested in \$300,000 online banking heist.** Turkish police have arrested an international gang that allegedly stole \$300,000 from online banking customers. Police in the Turkish city of Izmir have arrested 17 members of a gang who broke into online bank accounts, according to news reports. Law enforcement agencies have said the gang worked alongside three Russian hackers, who allegedly provided them with banking user names and passwords stolen through spyware planted on unwitting users' computers. The Russian hackers reportedly shared the password information of thousands of Turks in exchange for 10 percent of the stolen money. Source: <http://www.informationweek.com/showArticle.jhtml;jsessionid=C3YGIH0SNGSKQOSNDLOSJKH0CJUNN2JVN?articleID=197006766&articleID=197006766>

13. *February 15, InformationWeek* — **Massive insider breach at DuPont.** The Delaware U.S. attorney on Thursday, February 15, revealed a massive insider data breach at chemicals company DuPont where a former scientist late last year pleaded guilty to trying to steal \$400 million worth of company trade secrets. Gary Min worked as a research chemist for DuPont for 10 years before accepting a job with DuPont competitor Victrex in Asia in October 2005. Between August and December of that year, Min downloaded 22,000 sensitive documents and viewed 16,706 more in DuPont's electronic library, making him the most active user of that database in the company, according to prosecutors. It's unclear whether Min's frequent access to that database tipped off an automatic alert to DuPont officials or whether his behavior was

discovered by studying database access logs. The best way to guard against insider breaches is for companies to monitor database and network access for unusual activity and set thresholds that represent acceptable use for different users. If an employee starts downloading thousands of documents, and this is unusual for the job designation, this should automatically trip red flags to an administrator or manager.

Source: <http://www.informationweek.com/news/showArticle.jhtml?articleID=197006474>

[\[Return to top\]](#)

Transportation and Border Security Sector

14. *February 19, USA TODAY* — More dogs working air, rail security. More bomb-sniffing dogs than ever are patrolling the nation's airports and rail stations, and more are likely on the way as the federal government tries to blanket the nation's transportation hubs with highly visible security. The Transportation Security Administration (TSA) plans to add 45 dogs next year, primarily to subway and rail systems and also to the few large airports that don't have them. There are now 420 TSA-trained dogs patrolling 75 of the nation's largest airports and 13 major transit systems. On September 11, 2001, there were 174 dogs in 39 airports, according to TSA. The TSA wants to make canine teams so prevalent in transit hubs that suicide bombers would believe they'd be caught before they could strike. "They have phenomenal deterrent value," said Earl Morris, deputy chief of TSA's office of security operations. "We deploy them so people know that they're there." Dogs also can project a forceful image that reassures travelers. Tom Farmer, head of TSA's mass-transit division, told a recent rail-security conference. "They look good. They're imposing. They inspire fear about what the dogs can detect." In airports, dogs sniff cargo, luggage, passengers and planes. In rail stations, they focus on passengers and their bags.

Source: http://www.usatoday.com/travel/news/2007-02-18-security-dogs_x.htm

15. *February 19, Associated Press* — Fire kills at least 66 on India-Pakistan train; bomb suspected. Two bombs exploded on a train headed for Pakistan, sparking a fire that killed at least 66 people, in an attack officials said Monday, February 19, that was aimed at undermining the peace process between India and Pakistan. Dozens more people were injured. The explosion happened just before midnight on Sunday, February 18, in a rural area near Dewana in northern India. Most of the victims, officials said, were Pakistanis, using one of only two rail links between the neighboring rivals

Source: http://www.usatoday.com/news/world/2007-02-18-india-train_x.htm

16. *February 19, CNN* — Passengers safe after plane slides off Ohio runway. A passenger jet skidded off a runway and smashed through a fence while landing Sunday, February 18, in windy and icy conditions at Cleveland Hopkins International Airport. But none of the 70 passengers and four crewmembers were injured, a Federal Aviation Administration (FAA) spokesperson said. Shuttle America Flight 6448, which had taken off from Atlanta Hartsfield-Jackson International Airport, was landing in Cleveland when it left the end of Runway 28 and crashed through the fence, FAA spokesperson Laura Brown said. Although operated by Shuttle America, the flight was part of the Delta Connection network, spokesperson Warren Wilkinson said. "For reasons unknown, the plane did skid off the end of the runway, taking out a localizer antenna array used for that runway, going through a fence line," said

airport spokesperson Pat Smith.

Source: <http://www.cnn.com/2007/US/02/18/runway.mishap/index.html>

17. February 17, Associated Press — Airborne planes' windshields crack in blustery cold.

Airlines were investigating why windshields on at least 13 planes cracked at Denver International Airport as winds of up to 100 mph whipped through the foothills in Colorado. SkyWest Airlines reported cracked windshields on eight planes that were taking off or landing Friday, February 16, as winds gusted up to 50 mph, spokesperson Marissa Snow said. One plane's windshield cracked while it was airborne. "Only the outermost layer was affected," Snow said of the windshields, which are made from multiple layers of glass. SkyWest, a regional carrier for United Airlines, said the planes involved were the Embraer EMB120 Brasilia and Bombardier Canadair Regional Jet, though she did not immediately have numbers. Two Frontier Airlines Airbus planes had their windshields crack while airborne, while two other windshields cracked while at the gate, airline spokesperson Joe Hodas said. In all instances the planes returned to the airport and/or made it to the gate safely. No emergencies were declared and no injuries were reported. Spokesperson Steve Snyder said windshields cracked on several different makes and models of airplanes from several airlines, though he did not immediately know which and how many. None of the pilots reported flying debris, Snyder said.

Source: <http://www.cnn.com/2007/WEATHER/02/17/winter.weather.ap/index.html>

18. February 17, Pittsburgh Post-Gazette — Governor Rendell irate about Interstate 78 gridlock.

While ice-encrusted sections of three central Pennsylvania highways remained closed on Friday, February 16, an angry Governor Ed Rendell ordered an "immediate and complete" investigation to find out what had happened that resulted in hundreds of motorists being stranded in their cars for hours. At a news conference, Rendell said "significant mistakes in judgment were made" during Wednesday, February 14's severe ice and snow storm that jammed vehicles on Interstate 78, some for more than 24 hours, in the bitter cold. "There was a total breakdown in communication between state agencies," he said. The frozen parade of cars, SUVs, buses and trucks wasn't finally cleared off the road until Friday morning, but I-78 remained closed while Pennsylvania Department of Transportation crews put chemicals down and broke up several inches of ice from 50 miles of the road west of Allentown. The governor was upset about poor communications among PennDOT, the Pennsylvania Emergency Management Agency, the state police, and other agencies. He said he wants to find out why agencies weren't talking to one another as the storm worsened Wednesday and why no one contacted him about the dangerous backup on I-78 until 7:55 p.m. EST, more than 12 hours after the storm struck.

Source: <http://www.post-gazette.com/pg/07048/762899-85.stm>

19. February 16, Government Accountability Office — GAO-07-499T: Homeland Security: US-VISIT Has Not Fully Met Expectations and Longstanding Program Management Challenges Need to Be Addressed (Testimony).

The Department of Homeland Security (DHS) is investing billions of dollars in its U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program to collect, maintain, and share information on selected foreign nationals who enter and exit the United States. The program uses biometric identifiers (digital fingerscans and photographs) to screen people against watch lists and to verify that a visitor is the person who was issued a visa or other travel document. The program is also to

biometrically confirm the individual's departure. For over three years, the Government Accountability Office (GAO) has reported on US-VISIT capability deployments and shortfalls, as well as fundamental limitations in DHS's efforts to define and justify US-VISIT's future direction and to cost-effectively manage the delivery of program capabilities on time and within budget. GAO was asked to testify on (1) the status of the program's implementation and (2) the program's progress in addressing longstanding management weaknesses. Given where US-VISIT is today and the challenges and uncertainties associated with where it is going, GAO believes that DHS is long overdue in demonstrating that it is pursuing the right US-VISIT solution and that it is managing US-VISIT the right way.

Highlights: <http://www.gao.gov/highlights/d07499thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-499T>

- 20. February 16, Times Online (United Kingdom) — Quick-thinking pilot foils hijacker with the help of passengers.** The armed hijacker of an African aircraft was overpowered by passengers and crew Thursday evening, February 15, when the captain of the jet deliberately braked suddenly on landing in the Canary Islands. Ahmedou Mohamed Lemine, a 20-year veteran of Air Mauritania, realized during his conversations with the 31-year-old hijacker, who was seeking asylum in France, that his assailant did not speak French and that, on the moment of landing, he would be only person not wearing a seatbelt. So in the minutes before touching down at Gandó Airport, on Gran Canaria, Captain Lemine briefed his mainly-French speaking passengers and crew over the public address system that he would slam on the brakes as soon as he landed and then quickly accelerate, hoping to knock the man, who had two automatic pistols, off his feet. The plan worked and, according to Spanish officials, the hijacker, named as Mohamed Abderraman, tumbled over and dropped one of his guns before six men, including a Mauritanian mayor, stormed the pilot's cabin and threw a pot of boiling water on his groin and chest. The Spanish Interior Ministry said today that the Air Mauritania Boeing 737 took off from the Mauritanian capital, Nouakchott, yesterday evening carrying 71 passengers and a crew of eight

Source: <http://www.timesonline.co.uk/tol/news/world/europe/article1396430.ece>

- 21. February 16, ContraCostaTimes (CA) — Airport gates evacuated after security scare.** Authorities evacuated boarding gates at Oakland International Airport after a man set off a security checkpoint metal detector Thursday, February 15, and vanished, an airport spokesperson reported. About 1 p.m. PST, the alarm went off on a magnetometer at the security checkpoint for Terminal 2, said airport spokesperson Rosemary Barnes. "The passenger was not detained and proceeded to the boarding gate area," she said, adding that she did not know why or how the man avoided the normal security protocol of further screening. Airport authorities searched for the man, including on two flights that were boarding, but could find no one fitting the man's description, Barnes said. When the search proved fruitless, the airport evacuated the building, sending passengers to be rescreened in both terminals, Barnes said. The incident was similar to a January 5 security breach, in which a man darted into Terminal 2's passenger exit, prompting evacuation of both adjoining terminals. Just as in the earlier incident, none of the four entities responsible for airport security — Oakland police, Alameda County deputies, the Transportation Security Administration and the airport's privately security contingent — could find the interloper.

Source: http://www.mercurynews.com/mld/mercurynews/news/local/states/california/alameda_county/16712964.htm

22. *February 15, USA TODAY* — **NWA details its exit strategy.** Northwest Airlines (NWA) on Thursday, February 15, filed its long-awaited plan for getting out of Chapter 11 bankruptcy, promising to pay its unsecured creditors newly issued stock valued at about three-quarters of what they're owed. In a conference call with reporters, CEO Douglas Steenland said Northwest is on track to emerge from Chapter 11 before June 30. Steenland said the Eagan, MN-based carrier, still has "additional work to accomplish" while in Chapter 11, but that its restructuring work "positions Northwest well for future profits." The filing in a New York bankruptcy court answered many, but not all, of the key questions of how a reorganized Northwest plans to operate outside of Chapter 11. Northwest and Atlanta-based Delta filed for Chapter 11 protection on the same day in September 2005. Left unanswered for now: Northwest management's stake in a reorganized company.
Source: http://www.usatoday.com/travel/flights/2007-02-15-northwest-usat_x.htm

[\[Return to top\]](#)

Postal and Shipping Sector

23. *February 19, South Florida Business Journal* — **FedEx Ground opens Florida distribution center.** As part of its nationwide expansion plan, FedEx Ground has opened an automated distribution center in Pompano Beach, FL. FedEx said the 215,377-square-foot center will add more than 200 new jobs. The facility is triple the size of the two company operations in Fort Lauderdale and Pompano Beach that it replaces. The center has advanced package-sorting systems that can process 12,000 packages an hour.
Source: <http://biz.yahoo.com/bizj/070219/1420025.html?.v=1>

24. *February 16, Government Accountability Office* — **GAO-07-244: U.S. Postal Service: Vulnerability to Fluctuating Fuel Prices Requires Improved Tracking and Monitoring of Consumption Information (Report).** The U.S. Postal Service (the Service) is dependent on fuel to support its mail delivery and transportation networks, as well as to heat and operate the over 34,000 postal facilities it occupies. The Service has been challenged by recent fuel price fluctuations, and the Postmaster General stated that gas prices were a primary reason for the proposed 2007 postal rate adjustment. Based on this challenge, the Government Accountability Office (GAO) was asked to review (1) how the Service's fuel costs changed recently and the impact of these cost changes on the Service's financial and operating conditions, and (2) how the Service's actions to control fuel costs and mitigate risk compare to leading practices and federal requirements. GAO collected fuel cost and price information; interviewed Service fuel officials; and compared the Service's actions against leading practices and federal requirements. GAO recommends that the Postmaster General take actions to improve the Service's tracking and monitoring of transportation and facility-related fuel consumption data. GAO provided a draft of this report to the Service for its review and comment. The Service agreed with GAO's findings and recommendation and stated that it will take steps to improve its information systems that capture consumption data
Highlights: <http://www.gao.gov/highlights/d07244high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-244>

[\[Return to top\]](#)

Agriculture Sector

25. *February 19, Chicago Tribune* — **Canadian cattle slip past USDA safeguards.** Hundreds of cattle from Canada, which this month confirmed its ninth case of mad cow disease, have entered the U.S. without government–required health papers or identification tags, according to documents obtained by cattlemen in Washington state. The documents, consisting largely of correspondence between state officials and American cattle and meat companies, suggest problems with numerous truckloads of cattle that are shipped into the U.S. almost daily. Many of the documents note that cattle arrived in the U.S. without identification tags, or they had tag numbers that did not match the accompanying health certificates. Overall, the approximately 700 pages of records suggest that officials from Washington and possibly other states are having difficulty tracking hundreds of cattle that arrive from Canada each week. Ear tags that are supposed to be on cattle entering the U.S. from Canada are meant to track the cattle in case of an outbreak of disease or other problem. Health certificates confirm the health of cattle and also that they are under 30 months old, because young cattle are not thought to be fully vulnerable to mad cow. Together, the tags and health papers provide the major protection against sick cows coming into the country.
Source: http://www.chicagotribune.com/business/chi-0702190184feb19_1_2164665.story?coll=chi-news-hed
26. *February 17, Rockford Register (IL)* — **Five new CWD cases found in Illinois.** Tests have found five more chronic wasting disease (CWD) cases among hunter–harvested deer in northern Illinois. The state has had 168 confirmed cases since the first diseased deer was found near Roscoe in 2002. Twenty–one cases have been found since the start of the archery season last fall in Winnebago, Boone, DeKalb and McHenry counties. No new cases were discovered in Ogle County, which had its first cases the previous season. The total is expected to rise in coming weeks as Department of Natural Resources sharpshooters cull deer in known infected areas.
CWD information: <http://www.cwd-info.org/>
Source: <http://www.rrstar.com/apps/pbcs.dll/article?AID=/20070217/SPORTS1904/102170009/1155/SPORTS>
27. *February 16, Stop Soybean Rust News* — **First soybean rust of year in Texas found on soybeans.** Asian soybean rust was found Thursday, February 15, on old–crop and volunteer commercial soybeans in a field in Hidalgo County, TX — the farthest west rust has been found overwintering this year. The field near Monte Alto was harvested in December 2006. Rust was found on a handful of R6 plants the combine missed. A few pustules were found on volunteer plants (V2 to V3 stage). The field is scheduled to be disked soon and planted to sorghum. The over–wintering soybean rust sentinel plots planted at Weslaco, TX, are still in the vegetative stage.
Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=1021>
28. *February 16, Agricultural Research Service* — **Model predicts Rift Valley fever outbreak.** A Rift Valley fever outbreak was successfully predicted several months in advance for the first time with a model developed by a team assembled by an Agricultural Research Service (ARS) scientist. In October 2006, when the model predicted that Rift Valley fever would flare up

within three months in sub-Saharan Africa, a warning was sent to the United Nations Food and Agriculture Organization and the World Health Organization, which then passed on the warning to countries such as Kenya, Ethiopia, Tanzania, Uganda and Somalia. Rift Valley fever is primarily spread to livestock and humans by biting insects. The disease attacks cattle, sheep, camels and goats. Rift Valley fever has not reached the U.S., but having a model that can predict outbreaks allows the U.S. to know when to step up its own watch to prevent its spread to this country. The team included researchers from the Department of Defense's Global Emerging Infections System and the National Aeronautics and Space Administration's Goddard Space Flight Center. For the U.S. livestock industry, a Rift Valley fever outbreak would be devastating because the World Organization for Animal Health imposes a four-year ban on exports of beef, sheep or goat products from any country that has an outbreak.

Source: <http://www.ars.usda.gov/is/pr/2007/070216.htm>

[\[Return to top\]](#)

Food Sector

29. February 19, Associated Press — Grocery industry prepares for bird flu. Stocking up on food is as simple as a trip to the grocery store. But will household staples still be available if the U.S. is hit with a flu pandemic? Most people only have food on hand for three or four days. Unlike other critical infrastructure sectors, the food industry isn't getting much help from state and federal governments when it comes to disaster planning. That puts the burden on individual supermarket chains and wholesalers to deal with a potentially large number of sick workers that could affect store operations and disrupt the food supply. If a pandemic emerges, the U.S. Department of Homeland Security projects worker absenteeism to reach 40 percent or more over a prolonged period. The food and agriculture industry is listed among 13 critical-infrastructure sectors that the Department of Homeland Security says must remain functional during a pandemic. The Food Marketing Institute said a widespread pandemic will likely cause food consumption to shift away from restaurants and fast-food establishments and toward in-home eating, causing a greater demand for groceries. The federal government and public health agencies are urging people to stock up on nonperishable food, like canned goods and dried fruit, to ensure they have to food to eat during a pandemic.

Source: http://www.cbsnews.com/stories/2007/02/19/ap/business/mainD8_NCJ1L00.shtml

30. February 18, Associated Press — Feds to toughen meat, poultry inspection. The first major changes to food inspection in a decade will increase federal scrutiny of meat and poultry plants where the danger from E. coli and other germs is high or where past visits have found unsafe practices. The new policy will result in fewer inspections at plants with lower risks and better records for handling meat and poultry. To decide the level of scrutiny a plant should get, the "risk-based" system will consider the type of product and the plant's record of food safety violations. A plant that makes hamburger and has repeated violations would get more inspection. A plant that makes cooked, canned ham and has a clean track record would get less scrutiny. For now, the new system will be used in processing plants, not in slaughter plants. No timetable has been set for shifting to the new inspection system, although the Agriculture Department is expected to release one within the next few weeks.

Source: <http://www.businessweek.com/ap/financialnews/D8NCDCJ80.htm>

31. *February 18, U.S. Food Safety Inspection Service* — **Chicken strips recalled.** Carolina Culinary Foods, a West Columbia, SC, firm, is voluntarily recalling approximately 52,650 pounds of fully cooked chicken breast strips that may be contaminated with *Listeria monocytogenes*, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Sunday, February 18. The chicken breast strips were produced on January 9, 2007 and distributed to retail establishments nationwide. The problem was discovered through microbiological testing completed by the Georgia Department of Agriculture. FSIS has received no reports of illnesses associated with consumption of this product. Consumption of food contaminated with *Listeria monocytogenes* can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_012_2007_Release/index.asp
32. *February 16, U.S. Food and Drug Administration* — **FDA warns consumers not to use certain jars baby food.** The U.S. Food and Drug Administration (FDA) is warning consumers not to use certain jars of Earth's Best Organic 2 Apple Peach Barley Wholesome Breakfast baby food because of the risk of contamination with *Clostridium botulinum*, a bacterium which can cause botulism, a life-threatening illness or death. The affected product was sold in single individual jars and in variety packs. The food was distributed through retail stores and sold through the Earth's Best Website. If consumers have any of the specified jars in their home, they should not use it and destroy it immediately. No illnesses have been reported to FDA or the manufacturer to date in connection with this problem.
Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01566.html>
33. *February 16, Associated Press* — **Peanut butter plant probed in salmonella outbreak.** Government and company scientists went through one of the nation's largest peanut butter plants Friday, February 16, trying to figure out how salmonella got into batches of the spread. The plant has been shut down since Wednesday, February 14, when federal health officials linked its peanut butter — Peter Pan brand and certain batches of Wal-Mart's Great Value house brand — to a salmonella outbreak that has sickened almost 300 people nationwide since August. No deaths have been reported. It was unclear how the germ that commonly originates from the feces of birds and animals got into the peanut butter. Government and industry officials said the contamination may have been caused by dirty jars or equipment. Peanuts are usually heated to high, germ-killing temperatures during the manufacturing process. ConAgra says none of its previous routine testing of plant equipment and peanut butter has tested positive for salmonella. At least some the salmonella victims' peanut butter jars are being tested. Salmonella sickens about 40,000 people a year in the U.S. and kills about 600.
Source: <http://www.cnn.com/2007/HEALTH/02/16/peanut.butter.salmonella.ap/>

[\[Return to top\]](#)

Water Sector

34. *February 14, Los Angeles Business News* — **Mussel control program launched by Metropolitan Water Board.** A comprehensive program to detect and control an invasion of quagga mussels in the regional water import and treatment system that provides the Southland with half of its drinking water was launched Wednesday, February 14, by the Board of Directors of the Metropolitan Water District of Southern California. Quagga mussels, which are

related to the notorious zebra mussels that have overrun the Great Lakes and Mississippi River watershed, were found January 6 in Lake Mead, on the Colorado River, and were subsequently found at Metropolitan's Whitsett Intake Pumping Plant on Lake Havasu and the nearby Gene Wash Reservoir, at the beginning of the district's Colorado River Aqueduct. The mussels, which are spread by commercial ships and recreational boats, can multiply rapidly, clog pipes and pumping machinery, and ruin the ecology of lakes and reservoirs. The first phase of the program was approved unanimously by Metropolitan's board, and will be launched immediately with the purchase of \$180,000 of portable decontamination units, deep-water surveillance equipment, automated water samplers, and a \$16,000 polarizing microscope. It also includes increased surveillance of aqueducts and reservoirs by divers, and laboratory inspections of water samples.

Source: http://losangeles.dbusinessnews.com/shownews.php?newsid=107889&type_news=latest

[[Return to top](#)]

Public Health Sector

35. *February 19, Reuters* — Russia confirms bird flu outbreaks. Moscow's best-known pet market was in quarantine on Monday, February 19, as health officials confirmed a strain of H5N1 was responsible for five bird flu outbreaks around the Russian capital. Veterinary officials traced all five outbreaks, in separate villages around Moscow, to birds bought in the past two weeks at the capital's Sadovod market, commonly known as "Ptichka" ("Birdie"), where masked officials guarded empty stalls. Laboratory tests confirmed that the H5N1 bird flu present in all five cases was highly pathogenic and potentially dangerous to humans, said Nikolai Vlasov, head of veterinary surveillance at Russia's animal and plant health watchdog, Rosselkhoznadzor. The outbreak is Russia's second this year and the first ever recorded close to the capital. The H5N1 strain killed poultry in three settlements in the southern region of Krasnodar last month. No human cases of bird flu have been recorded in Russia.

Source: <http://www.alertnet.org/thenews/newsdesk/L19265631.htm>

36. *February 18, Boston Globe* — State moves to reduce use of emergency rooms.

Massachusetts officials will give four million dollars this year to community health centers in a new effort to steer patients with routine illnesses away from crowded hospital emergency rooms (ER). Twenty-one health centers in Boston and 11 other cities will use the money to open on additional nights and on weekends and pay for education campaigns to encourage patients to seek care at health centers rather than emergency rooms, for the flu, fever, sprains, backaches, nausea, rashes, cuts, and minor broken bones. The health centers also will expand capacity during regular hours, because data show that some patients go to the ER even when health centers are open. Many emergency room physicians said the initiative doesn't address the most pressing problem: back ups of seriously ill patients who need to be admitted to the hospital. The sickest patients can wait hours — even a day or longer — on gurneys in the ER, a situation caused in part by the elimination of nearly 40 percent of the state's hospital beds in the last two decades. Hospitals are taking other measures to attack this problem, such as discharging patients from rooms more quickly to free up beds.

Source: http://www.boston.com/yourlife/health/other/articles/2007/02/18/state_moves_to_reduce_use_of_ers/

37. *February 16, Agence France–Presse* — **Global database to open up access to bird flu virus genome.** A Swiss institute will shortly launch the world's first global, publicly–accessible database on strains of the H5N1 avian influenza virus, a virologist has said. The database at the Swiss Institute of Bioinformatics (SIB) is being set up in response to the Global Initiative On Sharing Avian Influenza Data (GISAID), launched last August by a group of 70 leading flu scientists and health officials. GISAID aims to overcome what it says a worrying failure to fully collect and share information about the bird flu virus. By failing to pool information about outbreaks or withholding data for commercial or personal gain, governments and scientists can badly hamper international efforts to tackle the disease, it warns.
Source: http://news.yahoo.com/s/afp/20070216/hl_afp/healthfluvirus_070216122856: ylt=AjEHNX6YjxwdUZXFfKBOesiJOrgF

[\[Return to top\]](#)

Government Sector

38. *February 17, Associated Press* — **Wisconsin Capitol building evacuated due to natural gas leak.** Utility officials have figured out how natural gas ended up in the Wisconsin Capitol building in Madison, WI, Friday, February 16, even though the building is heated by steam. Madison Gas and Electric spokesperson Steve Kraus says that the leak was in a natural gas coupling under a street less than a block from the building, and next to a telephone conduit that went into the Capitol. Someone reported a faint odor of natural gas in the Capitol basement just before 4:00 p.m. Friday. The building was evacuated as a precaution. Kraus says utility workers completed temporary repairs and the Capitol re–opened.
Source: <http://abclocal.go.com/wls/story?section=local&id=5043707>
39. *February 16, TMCnet* — **American School Bus Council bans cell phone usage by school bus drivers.** The American School Bus Council has exceeded a recent recommendation set forth by the National Transportation Safety Board (NTSB) on the use of cell phones by school bus drivers. The Council has prohibited the use of cellular phones or other portable electronic devices while driving. Even the devices equipped with hands–free devices are prohibited. The Council has also banned the use of cellular phones while supervising the loading and unloading of students. Although the Council recognizes that cellular phones and other communication devices can play a crucial role in emergency situations, it believes that these devices should be used only when the school bus is stopped and in a secure location, except in cases of extreme emergency. The Council released a set of guidelines on pupil transportation for use by those responsible for school transportation such as school districts, bus companies and pupil transportation officials on February 14. These guidelines provide clear national practices on bus driver qualifications, hiring and training; school transportation safety; emergency preparedness; and health and environmental safety.
Source: <http://www.tmcnet.com/news/2007/02/16/2344222.htm>
40. *February 16, Courant (CT)* — **Suspicious package found on school bus.** Police are investigating a suspicious package found on a Newington, CT, school bus Thursday afternoon, February 15, that brought out the Hartford police bomb squad and members of the Capital Region Hazardous Materials Team. The item, which was discovered at 4 p.m. EST in the

Newington school bus garage was packaged in a way that suggested it could be an explosive device, police said. Authorities later determined it was not explosive or had hazardous materials, but believe someone put the package on the bus to cause panic, police said. Investigators are working with school officials on the case.

Source: <http://www.courant.com/news/local/hc-newpackage0216.0.2084474.story?coll=hc-headlines-local>

41. *February 16, Department of Homeland Security* — **DHS forms partnership with NSF for Academic Research Initiative.** The Department of Homeland Security's (DHS) Domestic Nuclear Detection Office (DNDO) and the National Science Foundation (NSF) recently issued a potential \$58 million, over five years, in grant opportunities for colleges and universities that will focus on detection systems, individual sensors, or other research relevant to the detection of nuclear weapons, special nuclear material, radiation dispersal devices, and related threats. The program is called the Academic Research Initiative and will foster frontier research and build the nation's intellectual capital in nuclear sciences. "This Academic Research Initiative is a critical element in building the Nation's intellectual capital in nuclear detection capability," said DNDO Director, Vayl S. Oxford. "Continued advances in science and technology are a key element in the long-term effort to protect the Nation against nuclear attacks."

Source: http://www.dhs.gov/xnews/releases/pr_1171664755063.shtm

42. *February 15, Department of Homeland Security* — **DHS announces funding opportunities for additional Centers of Excellence.** The Department of Homeland Security's (DHS) Science and Technology (S&T) directorate announced on Thursday, February 15, \$12 million in funding opportunities that will establish four additional university-based Centers of Excellence in the areas of explosives detection, mitigation, and response; border security and immigration; maritime, island, and extreme/remote environment security; and natural disasters, coastal infrastructure, and emergency management. Managed by the S&T directorate's Office of University Programs, the Centers of Excellence leverage the capabilities of the nation's colleges and universities to conduct multidisciplinary research and education for homeland security solutions. The centers are authorized by Congress and chosen by DHS through a competitive selection process. The planned topics for the new centers match growing needs within DHS for basic, university-based, research.

Source: http://www.dhs.gov/xnews/releases/pr_1171579580231.shtm

[[Return to top](#)]

Emergency Services Sector

43. *February 19, Agence France-Presse* — **U.S. to stage world's largest anti-terrorism exercise on Guam.** The world's biggest anti-terrorism exercise will be held this year on Guam, underscoring the Pacific island's growing importance to the U.S. Exercise TopOff4 is part of a series of large-scale maneuvers established to strengthen the United States' ability to respond to terrorist attacks involving weapons of mass destruction. U.S. Coast Guard commander in Guam, William Marhoffer, said the TopOff4 exercise would be bigger than last year's Valiant Shield war games, in which the U.S. mobilized 30 ships, 280 aircraft and 22,000 military personnel. "It will be bigger in some ways. Valiant Shield was a military exercise. It was a show of force. It was the first time we had three carrier strike groups in combined operations in

the Pacific since the Vietnam War. "Top Officials (TopOff4) is a domestic counter-terrorism exercise ... it involves the intelligence communities, the Department of Homeland Security, the FBI, the Department of Defense, the U.S. Coast Guard." The exercise is expected to center around a maritime terrorist attack.

Source: <http://www.breitbart.com/news/2007/02/19/070219082113.b7gcc0 ha.html>

44. *February 15, Orange Bulletin (CT)* — **Mock disaster staged in Connecticut.** To evaluate its disaster preparedness, the town of Woodbridge, CT, held a mock disaster drill on February 10. The exercise was designed to require the set-up of a shelter. Along with the Woodbridge departments of Human Services and Police, Woodbridge also had the help of its Community Emergency Response Team. A group of volunteer ham radio operators helped with communications, which would be essential if there was a loss of telephone service. Volunteers serving as "displaced" persons were signed in and smoothly directed to appropriate areas by CERT members. Some "victims" spoke a foreign language or had a disability. Two young volunteers were asked to pose as troublemakers. Another was assigned the role of a drunk. These acts were staged to challenge the CERT volunteers and present them with some of the possible difficulties that might arise in a real disaster. A corner of the gym was set up for medical triage. This area was staffed by nurses, an emergency medical technician and other CERT members. After the drill was completed, the participants had a brief meeting to review the drill; a more extensive meeting will be held in the near future to review the drill process and address any problems.

Source: http://www.zwire.com/site/news.cfm?newsid=17854665&BRD=1661&PAG=461&dept_id=9538&rfti=6

45. *February 15, Indiana University* — **Indiana University Greek Council students training to become a Community Emergency Response Team.** Twelve representatives from the Indiana University Junior Greek Council will become the state's first Community Emergency Response Team (CERT) comprised solely of members of the Greek Community. The fraternity and sorority members have begun a five-week, 21-hour training course designed to prepare them to offer needed assistance in the case of a natural or man-made disaster. Funded by the Indiana Department of Homeland Security, CERT training covers areas of emergency preparedness including fire safety, light search and rescue techniques, basic disaster medical operations, first aid, cribbing and the principles of disaster psychology. The largest portion of the training provides the students with the skills necessary to triage disaster victims, set wounds and provide basic disaster response. The final class session ends with a practicum that puts the 12 IFC members' newly learned skills to use. The Bloomington Township Fire Department will light fires at its drill grounds so the students can practice extinguishing a fire, and there will be a mock disaster staged at one of the campus' 20 fraternity houses.

Source: <http://newsinfo.iu.edu/news/page/normal/4900.html>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

46. *February 16, US-CERT* — **Technical Cyber Security Alert TA07-047A: Apple Updates for Multiple Vulnerabilities.** Apple has released Security Update 2007-002 to correct multiple vulnerabilities affecting Apple Mac OS X, Mac OS X Server, and iChat. The most

serious of these vulnerabilities may allow a remote attacker to execute arbitrary code. Attackers may take advantage of the less serious vulnerabilities to bypass security restrictions or cause a denial of service. Apple Security Update 2007–002 addresses a number of vulnerabilities affecting Apple Mac OS X, OS X Server, and iChat. Further details are available in the related vulnerability notes. The vulnerabilities addressed in this update were previously disclosed as part of the Month of Apple Bugs project. The impacts of these vulnerabilities vary. Potential consequences include remote execution of arbitrary code or commands, bypass of security restrictions, and denial of service.

Users should install Apple Security Update 2007–002:

<http://docs.info.apple.com/article.html?artnum=106704>

Source: <http://www.us-cert.gov/cas/techalerts/TA07-047A.html>

47. February 16, US–CERT — Cisco Releases Security Advisories to Address Multiple Vulnerabilities in PIX, ASA, and FWSM.

Cisco has released Security Advisory cisco-sa-20070214-pix to address multiple vulnerabilities in the PIX 500 Series Security Appliances and the ASA 5500 Series Adaptive Security Appliances. The vulnerabilities exist due to flaws in the way Cisco PIX and ASA appliances process malformed HTTP requests, SIP packets, and TCP-based packets. By sending specially crafted packets to a vulnerable appliance, an attacker may be able to cause a denial of service, escalate user privileges, or take complete control of the appliance. Note: The Security Advisory also states that some of these vulnerabilities affect the Cisco Firewall Services Module (FWSM).

Cisco Security Advisory cisco-sa-20070214-pix – Multiple Vulnerabilities in Cisco PIX and ASA Appliances: http://www.cisco.com/en/US/products/products_security_advisory09186a00807e2484.shtml#details

Cisco Security Advisory cisco-sa-20070214-fwsm – Multiple Vulnerabilities in Firewall Services Module: http://www.cisco.com/en/US/products/products_security_advisory09186a00807e2481.shtml#details

Source: <http://www.us-cert.gov/current/#cscopxasa>

Internet Alert Dashboard

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

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

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

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 dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 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

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.