



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 22 February 2005

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

- The News Item reports vandalism to a piece of PPL equipment in Coal Township, PA, led to a power outage that left more than 11,000 utility customers in the dark for nearly two hours. (See item [1](#))
- The Associated Press reports ChoicePoint Inc. says that residents in all 50 states, the District of Columbia, and three U.S. territories may have been affected by a breach of the company's credentialing process in which criminals gained access to its massive database of consumer information. (See item [5](#))
- Georgia Tech Research News reports a Georgia Institute of Technology researcher recommends a systems engineering approach to homeland security that would include central command centers, response strategies tailored to a particular facility, and protection of water and air circulation systems in public buildings. (See item [42](#))

DHS/IAIP Update *Fast Jump*

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

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

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

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

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

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Products & 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://esisac.com>]

1. *February 21, The News Item (PA)* — **Authorities believe vandalism caused blackout.** Vandalism to a piece of PPL equipment in Coal Township, PA, led to a power outage that left more than 11,000 utility customers in the dark for nearly two hours Saturday, February 19.

Kathy Frazer, a spokesperson for PPL Corp., said that damage to equipment somewhere in the town impacted the utility's Fairview substation. Frazer did not know what piece of electrical equipment was vandalized. The outage, which occurred shortly before 10 p.m., lasted until approximately 11:50 p.m. Approximately 11,300 customers throughout Shamokin, Trevorton, parts of the Elysburg area and most of Coal Township were left in the dark, she said. Frazer said the utility is working with Coal Township police in investigating the incident.

Source: http://www.zwire.com/site/news.cfm?newsid=14000743&BRD=2311&PAG=461&dept_id=482260&rfti=6

2. *February 21, Associated Press* — **Anthracite coal shortage leaves homeowners scrambling.**

Coal yards in Schuylkill County, PA, the nation's number one producer of anthracite, say they are rationing coal to existing customers and telling new ones to look elsewhere. The culprit is lack of production. The shortage potentially affects thousands of homeowners who still heat with anthracite, a hard coal that is mined only in eastern Pennsylvania. Some worry that if the shortage persists, they'll have to convert to a more expensive kind of heat, like oil or gas. In Schuylkill County, the epicenter of the anthracite industry, coal processors say they are churning out far less than normal. Some have shuttered completely on days when there was not enough coal to start the plant. Coal taken from strip mines is readily available, but the recovery rate, or percentage of usable coal extracted from each ton of raw material, is a lot lower than it is for coal taken from deep mines. That's because there is a lot more dirt and rock mixed in, which means less coal processed during an eight-hour shift. The problem is largely confined to Pennsylvania, home to nine of the 10 counties with the highest percentage of households using coal for heating.

Source: http://www.miami.com/mld/miamiherald/business/national/10955_247.htm?1c

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

Chemical Industry and Hazardous Materials Sector

3. *February 21, Associated Press* — **Town's hazardous materials crews in good shape because of mill.** The director of the Idaho Bureau of Homeland Security says Lewiston, ID, has one of the best-developed hazardous materials response organizations in the state. William Bishop says part of that reason is the chemicals used at Potlatch Corporation's pulp and paper mill. Bishop says after the company once failed to report an unplanned release of chemicals, the company has improved its response by promptly reporting all spills. Within 15 minutes of a reported release, the company calls the state Department of Environmental Quality, the state Hazmat team, the Idaho Bureau of Homeland Security, and the North Central District Public Health Department. Bishop says the agencies discuss the leak and decide what action should be taken.

Source: <http://www.kbcitv.com/x5154.xml?ParentPageID=x5155&ContentID=x51828&Layout=KBCI.xsl&AdGroupID=x5154&URL=http://localhost/apwirefeed/d88csrjo0.xml&NewsSection=StateHeadlines>

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

Defense Industrial Base Sector

4. *February 19, Washington Post* — **Defense giants to buy information technology firms.** Two of the nation's largest defense contractors on Friday, February 18, announced plans to acquire information technology companies in their continuing drive to meet the government's growing demand for computer services as several major weapons systems face cuts. Northrop Grumman Corp. said it would acquire Chantilly, VA–based Integic Corp., which reported \$161 million in revenue last year — 90 percent of it coming from government contracts. The company's 600 employees, the majority of whom work in Chantilly, would become Northrop Grumman workers if the deal closes, as expected, this spring. Bethesda, MD–based Lockheed Martin Corp., which is the Pentagon's largest contractor, announced its planned purchase of Sytex Group Inc., in a \$462 million deal. The purchase would give Lockheed 3,000 new employees, 90 percent of whom have government security clearances. Sytex, based in Doylestown, PA, does about 85 percent of its work for the Department of Defense or intelligence agencies, Northrop Grumman said. Both deals follow the White House's fiscal 2006 budget proposal, which calls for an overall increase in military spending but cuts in some programs, such as Lockheed's F/A–22 Raptor fighter jet, and elimination of others, including a new generation of nuclear submarines.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A36768-2005Feb 18.html>

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

Banking and Finance Sector

5. *February 21, Associated Press* — **Company identity theft victims may be widespread.** ChoicePoint Inc. said Monday, February 21, that residents in all 50 states, the District of Columbia and three U.S. territories may have been affected by a breach of the company's credentialing process in which criminals gained access to its massive database of consumer information. ChoicePoint said it is almost done notifying by mail the 144,778 people that may have been affected. California authorities say as many as 500,000 people may have been affected, but ChoicePoint disputes that number. The company also announced that it is making roughly 17,000 customers go through a re-credentialing process to verify that they are legitimate businesses. Those customers that will have to be re-credentialed are any business that is not publicly traded or not a government agency. Once re-credentialed, those customers will no longer receive access to consumers' Social Security numbers, dates of birth and driver's license numbers unless they are sponsored by a public company or government agency, marketing director James Lee said. The company acknowledged last week that thieves apparently used previously stolen identities to create what appeared to be legitimate businesses seeking ChoicePoint accounts. The bandits then opened up 50 accounts and received volumes of personal data on consumers.

Source: <http://www.nytimes.com/aponline/business/AP-ChoicePoint-Identity-Theft.html>

6. *February 21, Reuters* — **Hacking attacks rarely made public, experts say.** A security breach that placed consumers at risk for identity theft grabbed headlines recently, but most hacking incidents go unreported to police or the public, experts said on Thursday, February 17. Afraid of negative publicity, most companies that suffer intrusions take a tight-lipped approach that leaves consumers unaware when their identities may be compromised, they said. At the same time, businesses are becoming more willing to discuss security issues with their competitors

behind the scenes in an effort to head off online threats, an approach experts say has managed to reduce the impact of computer worms and viruses. California is the only state that requires companies to notify consumers when an outsider is able to access their Social Security numbers or other information that puts them at greater risk for identity theft. Privacy experts said the California law paradoxically may discourage companies from examining intrusions too closely for fear that they might have to make them public.

Source: <http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=7690556>

7. *February 18, TechWeb News* — **New phishing tactic dangles millions as bait.** Phishers twisted a long-standing scam tactic into their newest technique to fake consumers out of their bank account information, a security firm said Friday, February 18. The new scheme starts with an e-mail from a phony bank, claiming that a large amount of money has been placed into a new account opened in the recipient's name. A link to the bogus bank is included, along with an account number and a PIN. The message goes on to say that the recipient can transfer the money by logging into this account and then by providing information about a real bank account to finalize the transfer. "We've seen phishers use fake banks before," said Dan Hubbard, the senior director of security at San Diego, CA-based Websense, "but this is the first time we've seen a scam that says money is waiting to be picked up." Hubbard said in explaining why this tactic doesn't use a real-world institution, as do many other phishing attacks, "More and more fraudulent-based sites are appearing that don't target a specific brand. ... Since the bank is probably fake, the phishers don't have to worry about any countermeasures. Who would someone report this to? There's no brand directly affected."

Source: <http://www.techweb.com/wire/security/60402291>

8. *February 18, Federal Computer Week* — **Officials from Colombia and the U.S. create finance database.** In a continuing effort to combat money laundering and other financial crimes, U.S. Immigration and Customs Enforcement (ICE) agents are working with Colombia's customs service officials to develop a joint database to exchange trade and financial information. Agents from ICE, which is part of the Department of Homeland Security, are helping Colombia's National Tax and Customs Directorate, or DIAN, to develop a Trade Transparency Unit. Officials from both agencies are developing an unprecedented joint database to exchange trade and financial information, according to an ICE press release. ICE agents also recently delivered 215 computers and other equipment to DIAN in that effort. Sharing information through this database will help agencies enhance Colombian officials' efforts to identify money laundering rings operating in both nations, according to the release.

Source: <http://www.fcw.com/fcw/articles/2005/0214/web-ice-02-18-05.a.sp>

9. *February 17, Reuters* — **Internet fraud threatens U.S. economy.** Internet fraudsters, motivated by money and armed with sophisticated technology, pose an increased economic threat as they steal private data from companies and individuals, the director of the U.S. Secret Service said on Thursday, February 17. "There is no longer any doubt about that threat ... With just a few key strokes, (online fraudsters) can disrupt our nation's economy," said Ralph Basham at a conference in San Francisco, CA. Security analysts have warned that Internet hackers, once motivated by the thrill of shutting down computer systems, are joining forces with organized crime groups as they seek to profit from hacking into databases and stealing personal data through a variety of tactics. Increased cooperation and information sharing between U.S. agencies, foreign governments, technology companies and the financial

community has helped mitigate online fraud, Basham said. Howard Schmidt, a special advisor for cyberspace security during the first term of President George W. Bush, said companies and individuals are better protected now than ever before and are also more aware of online fraud risks. However, he cautioned that Internet fraudsters were increasingly targeting less-protected small businesses rather than large companies that can spend millions of dollars on security software to protect their computer systems.

Source: <http://www.reuters.com/financeNewsArticle.jhtml?type=bondsNews&storyID=7667753>

10. *February 16, PC World* — **New phishing attack outsmarts typical defenses.** Phishers have found a new way to snare data without users clicking a link. The new phishing scam works when users receive an HTML e-mail message, and open (or even just preview) the message in the e-mail client software. Windows PCs lacking one particular Microsoft security patch will run a tiny JavaScript applet as the client renders the HTML. The QHosts Trojan horse applet modifies the PC's Hosts file so that when a bank's URL is typed, the user actually goes to a site controlled by the fraudsters. Since phishers have gotten very good at mimicking real sites, one may never know you're at the wrong site. While the impact of QHosts has been limited so far, phishers are likely to use this new technique much more in the near future. The fact that the Hosts file is easy to protect will be cold comfort to future victims who get hit with the next QHosts-like phishing scam.

Source: <http://www.pcworld.idg.com.au/index.php?id=1112929253>

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

Transportation Sector

11. *February 20, Denver Post* — **Denver airport officials concerned about United's future.**

After ten years of operation, Denver International Airport's (DIA) successes are apparent in the numbers: DIA handled a record 42.4 million passengers in 2004, solidifying its place as the nation's fifth-busiest airport. It also has lived up to its billing as one of the world's most efficient, spacious and technologically advanced airports. In 2004, it had the highest percentage of flights arriving on time among major U.S. airports. Nevertheless, DIA still is weighed down with \$4 billion in debt, high operating costs for airlines, and a dependency on United Airlines. United and its commuter affiliates handle about 59 percent of DIA's passengers. The Denver airport is United's second-largest hub, after Chicago's O'Hare International Airport. Chicago-based United, which has lost a staggering \$9.7 billion over the past four years, filed for bankruptcy in December 2002. If negotiations between United and its unions fail and workers act on their threats to strike the carrier, it could kill the airline. The death of United would be catastrophic for Denver's airport. At this point, uncertainty over United's future — and the overall condition of the industry — have forced DIA to shelve hundreds of millions of dollars in planned capital improvements.

Source: <http://www.denverpost.com/Stories/0.1413.36%7E33%7E2720416.0.0.html>

12. *February 19, Des Moines Register (IA)* — **Air control tower at Des Moines airport not on cutback list.** The Des Moines airport has been dropped from a list of airports across the nation that are being considered for reduced air traffic control operations under a government cost-cutting plan. Control towers at 48 midsize airports would be closed between midnight and

5 a.m. each day under a recently reported Federal Aviation Administration (FAA) plan. The Des Moines airport was among the airports on that list. But aides to Sen. Charles Grassley, R-IA, said they contacted the FAA Friday, February 18, and learned that Des Moines no longer was on the list. FAA spokesperson Greg Martin said the agency is looking to adjust staffing in its control towers to meet changes in demand. The FAA has not made a final decision on the cutbacks and is reviewing each airport, he said. Airports under review handle few commercial and cargo flights during those late-night hours. Federal air traffic controllers staff 315 airports, but not all are operated around the clock. In addition, there are 193 airports with scheduled commercial air service that do not have control towers, Martin said. When a tower is empty, pilots are always in voice contact with a controller elsewhere in the region, Martin said.

Source: <http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20050219/BUSINESS04/502190318/1029/BUSINESS>

13. *February 19, Associated Press* — **District hazardous train ban could heighten risks in other CSX states.** A newly passed ordinance barring rail shipments of hazardous materials through the District of Columbia raises the risk of a catastrophic accident or terrorist attack in Maryland and other states with CSX lines as the dangerous cargo is rerouted around the nation's capital, railroad officials say. CSX Corp., the train operator most affected by the law that Washington Mayor Anthony A. Williams signed Wednesday, February 16, says that unless the measure is reversed, it will likely cause backups and bunching of chemical tank cars at its rail yards in Baltimore, Cumberland, MD, Philadelphia, and Richmond, VA — places where hazardous cargo would be segregated and diverted to outlying routes, including through Tennessee. Two trade groups, the Association of American Railroads and the National Industrial Transportation League, concurred with CSX and added in separate filings that the need for emergency preparedness would increase in small cities along hundreds of miles of alternate, less suitable rail lines. "These consequences of forcing traffic over alternate routes are likely to actually increase exposure — and therefore reduce safety and security — as well as imposing added costs on our economy," the Association of American Railroads officials said.

Source: <http://pennlive.com/newsflash/pa/index.ssf?/base/news-24/11088329973591.xml&storylist=penn>

14. *February 19, Des Moines Register* — **Licenses rejected for those in Iowa illegally.** The Iowa Supreme Court ruled Friday, February 18, that people who are in the United States illegally have no constitutional right to a driver's license. The decision strengthened opponents' arguments that granting licenses to undocumented people poses a security risk and rewards an illegal act. Advocates for the licenses, though, warned that thousands of illegal immigrants will continue to drive in constant fear of law enforcement and without insurance, increasing costs for everyone. The unanimous ruling said Iowa's license requirements are in place so that "governmental machinery" is not "a facilitator for the concealment of illegal aliens." Justices also said the issue should be decided by state lawmakers, and advocates immediately vowed to turn their attention to the state Capitol. Ten states, including Illinois and Wisconsin, permit driver's licenses for immigrants in the country illegally.

Source: <http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20050219/NEWS10/502190330/1001>

15. *February 19, Associated Press* — **Metro asks for more federal funds.** At a hearing on Capitol Hill, on Friday, February 18, Metro Board Chair Dana Kauffman asked the federal government

to play a bigger role as the transit agency attempts to secure a steady stream of revenue to maintain current levels of service, as well as expand. "It's important to note that we added 10,000 new daily riders in December " a strong sign that we're doing something right," said Kauffman, who represents Fairfax County, VA, on the board. He noted that many Metro riders are federal employees and said the government should do more to cover the system's costs. But Rep. Thomas M. Davis III, Virginia Republican and chairman of the House Government Reform Committee, said lawmakers must take a closer look at how well Metro is run. Davis rattled off a list of problems in the past year: revelations that millions of dollars in parking revenue had gone missing, a train wreck at the Woodley Park station, and difficulties with the SmarTrip card program. To improve its image, Metro has announced a series of initiatives aimed at improving customer service, reliability and safety.

Source: <http://washingtontimes.com/metro/20050218-103515-6338r.htm>

16. February 19, Lincoln Tribune (NC) — Financing to provide liquidity during restructuring.

US Airways Group, Inc., on Saturday, February 19, announced that it has reached agreement with Eastshore Aviation, LLC, an investment entity owned by Air Wisconsin Airlines Corp., and shareholders, on a \$125 million financing commitment to provide a substantial portion of the equity funding for a plan of reorganization. The \$125 million facility will be made in the form of a debtor-in-possession term loan, to be drawn in the amount of \$75 million (immediately upon approval by the U.S. Bankruptcy Court) and two subsequent \$25 million increments. This loan would be second only to the Air Transportation Stabilization Board loan with regard to the company's assets that are pledged as collateral. Upon emergence from Chapter 11, the \$125 million financing package would then convert to equity in the reorganized US Airways. Air Wisconsin, based in Appleton, WI, is the nation's largest privately held regional airline. In 2004, its 87 all-jet fleet generated approximately \$700 million in revenue and flew more than seven million passengers under the United Express brand. As part of this agreement, US Airways and Air Wisconsin will enter into an air services agreement under which Air Wisconsin may, but is not required to, provide regional jet service under the US Airways Express brand.

Source: http://www.lincolntribune.com/modules/news/article.php?story_id=804

17. February 19, Washington Post — FAA issues directive on business jet.

The Federal Aviation Administration (FAA) has directed operators of the Canadair Challenger 600-series business aircraft to more carefully inspect the plane's wings for ice and frost before takeoff, after two accidents involving the aircraft in the past three months. A Challenger 600 aircraft, one of the most popular jets among corporate executives and charter operators, crashed in Colorado in November, killing the son of NBC executive Dick Ebersol, a flight attendant and one of the pilots. The aircraft was also involved in an accident three weeks ago at New Jersey's Teterboro Airport, in which the pilot was unable to get off the ground and crashed into a warehouse. Flight manuals for the aircraft will be changed so that a pilot or co-pilot must run their hands along the wing's leading edges to inspect for frost, ice or snow. Previous manuals required only a visual inspection of the wing, according to a spokesperson for Bombardier Inc., which acquired Canadair. Bombardier, which still sells the Challenger, said it agreed with the FAA's instruction but also defended the plane's safety record.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A36531-2005Feb 18.html>

18.

February 19, Associated Press — **Truck driver shortage affecting consumers.** Trucking is an industry where driver turnover is growing and consumers are facing longer delays and higher prices for food, clothes and thousands of other products that must be trucked each day. Consultant Lana Batts said the industry already is 195,000 drivers short of what it needs. "It is a very tough, demanding job: long hours, significant time away from home, increased road congestion, an increase in regulation," said Scott Arves of Schneider National Inc. The increased costs of recruiting new drivers, plus higher fuel prices, can add pennies to the cost of a gallon of milk and dollars to a plasma television set. Security requirements have only exacerbated the shortage, drivers and analysts say. Hauling fuel and other hazardous substances used to require little more than a clean driving record and some training. Now, due to security regulations, drivers who want to transport such materials have to undergo a background check and fingerprinting. In addition, new regulations designed to ensure that tired truck drivers aren't on the road have forced a lot of them to sit at rest areas unable to deliver or pick up their loads. Source: <http://www.clarionledger.com/apps/pbcs.dll/article?AID=/20050219/BIZ/502190367/1005>

19. *February 19, Star-Telegram (TX)* — **Suspect's gear set off airport alarms.** The bag of a man who was arrested at a Detroit airport after saying he was headed for Syria to try to claim the \$25 million bounty for Osama bin Laden set off security alarms at Dallas/Fort Worth Airport (D/FW) on Tuesday, February 15, a transportation security official said Friday, February 18. Inside Matt Mihsen's bag, D/FW screeners found a stun gun, pepper spray, two boxes of Black Talon 9 mm ammunition, a bulletproof vest and three Geiger counters. None of the items is banned from checked luggage, so they were inspected for explosive residue and repacked, and the bag was placed on Mihsen's Northwest Airlines flight to Detroit, said Andrea McCauley, a spokesperson for the Transportation Security Administration. Before he boarded an international flight from Detroit to the Netherlands en route to Syria, customs and border protection officers pulled Mihsen aside for questioning, according to an affidavit for his arrest. He was found to be carrying \$13,756, the affidavit states. Mihsen faces charges of lying to federal investigators, attempting to smuggle bulk cash out of the United States and attempting to export goods and money to Syria in violation of a presidential order. Source: <http://www.dfw.com/mld/startelegram/news/local/10942792.htm? 1c>

20. *February 18, Government Accountability Office* — **GAO-05-198: Border Security: Streamlined Visas Mantis Program Has Lowered Burden on Foreign Science Students and Scholars, but Further Refinements Needed (Report).** In February 2004, the Government Accountability Office (GAO) reported that improvements were needed in the time taken to adjudicate visas for science students and scholars. Specifically, a primary tool used to screen these applicants for visas (the Visas Mantis program) was operating inefficiently. GAO found that it took an average of 67 days to process Mantis checks, and many cases were pending for 60 days or more. GAO also found that the way in which information was shared among agencies prevented cases from being resolved expeditiously. Finally, consular officers lacked sufficient program guidance. This report discusses the time to process Mantis checks and assesses actions taken and timeframes for improving the Mantis program. GAO recommends that the Secretary of State, in coordination with the Secretary of Homeland Security, (1) develop a timeframe for connecting agencies to the Mantis tracking system; and (2) provide officers at key posts more opportunities to learn through direct interaction. In response, the Departments of State and Homeland Security said they are implementing the recommendations.

Highlights: <http://www.gao.gov/highlights/d05198high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-05-198>

21. *February 18, Federal Computer Week* — **Fingerprint standard still elusive.** Two months after a Justice Department inspector general warned of stalled progress on interoperable fingerprint systems, no settlement has been reached on a uniform fingerprint technology standard. According to a December 2004 Justice inspector general report, progress toward making all biometric fingerprint systems fully interoperable has stalled, partly because Justice, the Department of Homeland Security and the State Department had not agreed on a uniform fingerprint technology standard. Currently, immigration and criminal fingerprint systems do not share information, which prevents immigration officials from recognizing criminals and wanted aliens in their custody. The number of fingerprints each system collects is part of the loophole. The FBI uses a 10-fingerprint system, called the Integrated Automated Fingerprint Identification System, or IAFIS. The Homeland Security Department uses a two-fingerprint system, called IDENT, for the U.S. Visitor and Immigrant Status Indicator Technology program. In addition, the National Institute for Standards and Technology (NIST) recommends 10 fingerprint images for US-VISIT enrollment in its NIST Patriot Act Recommendations, citing accuracy. State contends that additional prints would slow down travel and increase costs.

Source: <http://www.fcw.com/fcw/articles/2005/0214/web-fingers-02-18-05.asp>

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

Postal and Shipping Sector

22. *February 19, Reuters* — **Syringes sent to British embassy seized.** Syringes were sent to Great Britain's embassy in Moscow, Russia, in a package that was intercepted by security staff, the Foreign Office said. Police are examining the syringes and the Foreign Office is taking the matter seriously, said a spokesperson on Friday, February 18. "Our embassy in Moscow received several packets. There were four packets and only one of them contained syringes that were revealed by security checks," said the spokesperson. The other three packages contained papers. Several embassies of the U.S. and other countries have been forced to close temporarily over past months after receiving envelopes containing white powder.

Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=topNews&storyID=2005-02-18T133113Z_01_CUT848380_RTRUKOC_0_SECURITY-BRITAIN-MOSCOW.xml

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

Agriculture Sector

23. *February 19, Associated Press* — **Popular veterinary manual updated.** As a veterinary student in the 1980s, Ira Roth often carried the Merck Veterinary Manual in his back pocket. But today's students can't stuff the latest edition into any pocket -- it has 2,712 pages and weighs three pounds. To keep up with the world's emerging animal-to-human diseases and growing bioterrorism threats, the reference book's first update in seven years has 35 more

chapters and 400 more pages than the previous manual. The ninth edition reflects enormous changes in veterinary fields in recent years: outbreaks of animal diseases that also threaten humans, like bird flu, monkeypox, and West Nile; growing concerns that cattle and other livestock could be used by terrorists to poison the nation's food supply; and advances in pain management and disease diagnosis. The editors also expanded the book's coverage of anthrax, a naturally occurring bacterium that typically affects sheep and cattle.

Source: <http://www.rednova.com/news/display/?id=129240>

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

Food Sector

24. *February 18, Kentucky Department of Agriculture* — Contaminated eggs may have been sold in Kentucky. The Kentucky Department of Agriculture (KDA) urges consumers to be on the lookout for potentially contaminated eggs from an Ohio packing plant that may be on retailers' shelves or in homes in the eastern half of the state. The eggs were distributed under several different labels. Between 60 and 300 cases of eggs, containing 15 dozen eggs in each case, were shipped to stores between Ashland and Louisville and from the Ohio River to the Tennessee border. KDA inspectors caught about half of the suspected contaminated eggs and are tracking the rest. Department officials believe many of the cartons already have been sold to consumers. Department egg inspectors discovered the potentially contaminated eggs while performing routine egg inspections.

Source: http://www.kyagr.com/news_events/eggalert.htm

25. *February 16, Food and Drug Administration* — Salmon recalled. Florida Agriculture and Consumer Services Commissioner Charles H. Bronson Wednesday, February 16, announced that Florida Smoked Fish of Miami is recalling its packages of The Boy's Farmer Market brand of "Smoked Nova Salmon" because it has the potential to be contaminated with *Listeria monocytogenes*. The recalled salmon was distributed nationwide. No illnesses have been reported to date in connection with this problem. The contamination was noted after testing by the Florida Department of Agriculture and Consumer Services revealed the presence of *Listeria monocytogenes*. Production of the product has been suspended while the company continues its investigation as to the source of the problem.

Source: http://www.fda.gov/oc/po/firmrecalls/farmermarket02_05.html

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

Water Sector

26. *February 18, Environmental Protection Agency* — EPA sets reference dose for perchlorate. The Environmental Protection Agency (EPA) has established an official reference dose (RfD) of 0.0007 mg/kg/day of perchlorate. A reference dose is a scientific estimate of a daily exposure level that is not expected to cause adverse health effects in humans. EPA's reference dose for perchlorate will be posted on the agency's online IRIS database, which contains risk information on possible human health effects from exposure to chemical substances in the environment. EPA's new RfD translates to a Drinking Water Equivalent Level (DWEL) of 24.5

ppb. A Drinking Water Equivalent Level, which assumes that all of a contaminant comes from drinking water, is the concentration of a contaminant in drinking water that will have no adverse effect with a margin of safety. Because there is a margin of safety built into the RfD and the DWEL, exposures above the DWEL are not necessarily considered unsafe. Perchlorate has been detected in drinking water in some systems around the country. The perchlorate summary is available at: <http://www.epa.gov/perchlorate>

Source: <http://yosemite.epa.gov/opa/admpress.nsf/b1ab9f485b098972852562e7004dc686/c1a57d2077c4bfda85256fac005b8b32!OpenDocument>

[[Return to top](#)]

Public Health Sector

27. *February 21, Associated Press* — School nurses not ready for terror attacks. School nurses nationwide say they need to be more prepared for emergencies such as terrorist attacks. Nearly half the nurses who responded to a National Association of School Nurses survey listed emergency preparedness as their highest priority. But, disaster preparedness trainer Deborah Strouse noted that many schools don't even have a full-time nurse or health services. Schools were recognized as potential terrorist targets long before the seizure of a Russian school in September in which 330 hostages were killed. The National Association of School Nurses, which has about 12,500 members, has developed a disaster preparedness program to meet the demand for training -- more than 2,000 school nurses have participated.

Source: <http://www.kansascity.com/mls/kansascity/news/local/10953220.htm?l>

28. *February 21, Agence France Presse* — Mystery illness shuts Australian airport terminal for hours. One of Australia's main airport terminals was shut down for eight hours as emergency crews hunted in vain for the cause of a mystery illness which struck down nearly 60 staff and passengers in the building, officials said. Paramedics, firefighters and hazardous materials crews in full protective clothing rushed to Melbourne airport Monday, February 21, after staff in a domestic terminal began suffering nausea and vomiting, dizziness, headaches, and shortness of breath. Up to 2,000 staff, passengers and their friends were evacuated and the terminal shut down around 10:00 a.m., while emergency crews tested air conditioning units and other facilities in an unsuccessful search for what was causing the illness. Those affected were mostly security and airline staff working in the departure area for domestic carrier Virgin Blue, officials said. The shutdown of the terminal caused chaos around the airport, forcing the cancellation or postponement of scores of Virgin Blue and other domestic flights. A Virgin Blue spokesperson said the terminal reopened at 6:00 p.m., and flights resumed about two hours later. While some kind of toxic gas was the main suspect in the incident, the exact cause of the contamination remained a mystery.

Source: http://www.channelnewsasia.com/stories/afp_asiapacific/view/133627/1.html

29. *February 20, BBC News* — Threat of new SARS outbreak low. The world is unlikely to face an explosive Severe Acute Respiratory Syndrome (SARS) outbreak like the one of two years ago, say experts. The strain of the virus that jumped readily between humans probably only exists in lab samples, they believe. It would take an unhappy accident or a fresh mutation of the virus in an animal host for it to re-emerge, a science meeting in Washington, DC, heard. And even if it did, it could be quickly contained, said Kathryn Holmes from Colorado University.

She said scientists had learned a great deal from the epidemic of SARS that began in November 2002 and ended in June 2003. "We now have wonderful, very sensitive diagnostic tests and new treatments to fight any outbreak. A number of labs have human monoclonal antibodies that neutralize SARS virus. These might be used to treat infected individuals or protect the healthcare workers around them. There are also multiple vaccine candidates for SARS that have been developed," she told the annual meeting of the American Association for the Advancement of Science.

Source: <http://news.bbc.co.uk/1/hi/health/4280253.stm>

30. *February 20, Reuters* — **West Africa launches anti-polio drive.** Three West African countries at the center of a polio epidemic launched an immunization drive on Sunday, February 20, to help stop the spread of the disease by the end of this year. A boycott of the vaccine by Muslim leaders in northern Nigeria led to a doubling in the number of Nigerian children paralyzed by polio to 788 in 2004, and helped spread the virus to 12 African countries previously declared polio-free. Immunizations resumed eight months later after northern political leaders, under intense international and domestic pressure, agreed to re-examine the scientific evidence. The presidents of Nigeria, Benin, and Niger launched the new initiative, which will cover 23 African countries. Nigeria, Africa's most populous country which accounted for two-thirds of the world's new polio cases last year, plans an intensive immunization campaign this year comprising five separate rounds aimed at 40 million children.

Source: <http://olympics.reuters.com/newsArticle.jhtml?type=healthNews&storyID=7681364>

31. *February 19, Canadian Press* — **New Canadian disease center.** Canadian health officials expressed confidence Friday, February 18, that Canada is ready for the next infectious disease outbreak as they officially opened a new emergency operations center. The center includes a video screen along with computers and a bank of telephones. It will allow health officials to hold videoconferences and share computer data with counterparts across the country and with international groups such as the World Health Organization. In the event of an outbreak, the technology would also allow researchers at the nearby National Microbiology Lab to develop vaccines in conjunction with researchers in other countries, said Frank Plummer, the lab's scientific director general.

Source: <http://www.canada.com/health/story.html?id=108cf8d0-8c6d-47da-86e4-106001cb3643>

32. *February 19, Associated Press* — **Congo plague outbreak.** A rare form of plague has killed at least 61 at a diamond mine in the northeast Congo, and authorities fear hundreds more who fled into the forests to escape the contagion are infected and dying, the World Health Organization (WHO) said Friday, February 18. Eric Bertherat, a doctor for the WHO, said the outbreak has been building since December around a mine near Zobia. Nearly all the 7,000 miners have abandoned the infected area and sought refuge in the world's second-largest tropical rain forest, all but cut off from the outside world. Security fears — mainly from bandits and militia leftover from Congo's five-year war — have also slowed international response, Bertherat said. Bertherat, speaking to reporters by telephone, said plague is commonly found in this region of northern Congo, but this large an outbreak was unusual.

Source: <http://www.cnn.com/2005/HEALTH/02/18/congo.plague.ap/index.html>

33.

February 18, Food and Drug Administration — **New product to treat complications of smallpox vaccination approved.** The Food and Drug Administration (FDA) has approved Vaccinia Immune Globulin Intravenous (VIGIV) — the first intravenous human plasma–derived product available to treat certain rare complications of smallpox vaccination. VIGIV is made from the pooled plasma of donors who received booster immunizations with the licensed smallpox vaccine — Dryvax. This plasma contains increased levels of protective antibodies against the vaccinia virus, the live virus used in the currently available smallpox vaccine. The vaccinia virus is similar to the smallpox virus, but does not cause smallpox. Because the smallpox vaccine is made with this live virus, even though it is a weakened virus, occasionally it can cause infections in susceptible vaccinated people or those in close contact with them. People with weakened immune systems or certain skin conditions are susceptible to vaccine complications. VIGIV helps treat these complications.
Source: <http://www.fda.gov/bbs/topics/ANSWERS/2005/ANS01341.html>

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

Government Sector

Nothing to report.

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

Emergency Services Sector

34. *February 21, Baltimore Sun (MD)* — Better weather data aid safety. The Maryland Emergency Management Agency (MEMA), local police and fire officials are using weather data collected 24 hours a day by WeatherBug, a commercial weather service provider. The fee paid by the state also provides data access for all county emergency managers and first responders in Maryland, said Warren Campbell, deputy director of technical support at MEMA. Its chief selling point is the density of its weather network. No Marylander lives far from one of its 300 stations. Most were built at schools in exchange for free access to the data by math and science classes. Integrated weather data from the National Weather Service, the Department of Transportation, and WeatherBug's 300 stations is accessed using digital maps displayed on PCs and a projected screen at the state's Emergency Operating Center in Reisterstown. The maps can be combined with other systems to show how the weather data relate to population densities, evacuation routes, hospitals, firehouses and sites housing hazardous materials. In the event of a spill, MEMA officials would feed in data, such as wind speed, direction and humidity, then add the chemical and its transport characteristics, and generate a map of the areas most at risk.

Source: <http://www.baltimoresun.com/news/local/bal-md.weatherbug21feb21.1.4045030.story?coll=bal-local-headlines&ctrack=1&cset=t rue>

35. *February 20, Philadelphia Inquirer (PA)* — Firefighters make a dry run for danger. In a field near the Gloucester County, PA, Fire Academy, a dozen firefighters stood back recently as a white vapor, sparked by a torch, ballooned into a 40-foot flame. Ignited were 2,000 gallons of liquefied natural gas (LNG), a product that BP wants to ship by tanker to a site a few miles away. Tankers, however, would carry millions of gallons — a potential terrorist target. The

firefighters, part of a task force of first responders that formed after BP announced its plans, were trying to assess their ability to fight an LNG–fueled fire. Using handheld extinguishers, three firefighters sprayed streams of retardant on the fire. It recoiled briefly but surged back to full force. On the second try, the men doused it, but it quickly reignited. The third attempt worked. At the training session, sponsored by BP at the request of the task force, the firefighters learned that LNG burns faster and hotter than gasoline and propane and can be extinguished with a dry fire–retardant agent called Purple K. James Fay, an LNG expert and emeritus professor at the Massachusetts Institute of Technology, has said that with a massive LNG tanker blaze, "there's no possibility you could put out one of these fires."

Source: <http://www.philly.com/mld/inquirer/news/nation/10943752.htm? 1c>

- 36. February 19, *The Arizona Republic* — Emergency response team ready in Foothills.** Should a large–scale disaster, such as a terrorist attack, strike in Phoenix, AZ, 76 city residents are now trained to provide assistance. These residents, skilled in disaster preparedness and disaster medicine, are the first members of the Community Emergency Response Team (CERT) of Phoenix. The U.S. Department of Homeland Security is building a nationwide network of these teams, including 30 in Arizona, in response to the 2001 terror attacks. The purpose is to supplement first responders, such as fire and police officials, in the case of terror attack, natural disaster, train derailment or other major emergency, and to get citizens engaged in contingency planning. Those who complete the initial 20 hours of training may go on to Tier 2, a higher level that requires an additional 60 hours of training specific to the Phoenix area, such as how to respond to a monsoon, blackout, flood or dust storm emergencies. With another 60 hours of training, volunteers will be given Tier 3 certification and official city volunteer status. Within five years, the city hopes to have about 13,000 trained CERT members: 8,000 in Tier 1, 4,000 in Tier 2 and 800 in Tier 3.

Source: <http://www.azcentral.com/community/ahwatukee/articles/0219ar-cert19Z14.html>

- 37. February 19, *The Advocate (CT)* — Connecticut security chief seeks teamwork.** First responders from Fairfield County, CT, gathered at Westport Town Hall on Friday, February 18, for a briefing on the state's newly created Department of Emergency Management and Homeland Security. Addressing the group of more than 100 police, fire and public officials was state Homeland Security director–designate James "Skip" Thomas, who talked about how much the new department will depend on local knowledge to keep the state safe. "Our goal is to prevent something from happening. The whole issue for me is prevention, prevention, prevention," Thomas said, adding that information traveling one way -- upward -- from local to state officials won't get the job done. "If we can intervene early, we can mitigate things happening. The only way we can do that is by sharing information," Thomas said. At the beginning of this year homeland security was combined with the state's emergency management operations to form the Department of Emergency Management and Homeland Security. Westport Fire Chief Denis McCarthy said consolidating the state's emergency management and homeland security efforts was a smart way to make citizens safer.

Source: <http://www.stamfordadvocate.com/news/local/scn-sa-nor.emergency4feb19.0.6716018.story?coll=stam-news-local-headlines>

[[Return to top](#)]

Information Technology and Telecommunications Sector

38. *February 20, NewScientist* — **Novel cryptographic protocol could help secure wireless computer networks.** Markus Jakobsson and Steve Myers of Indiana University demonstrated a new security scheme, dubbed "delayed password disclosure," at the American Association for the Advancement of Science meeting in Washington, DC, on Saturday, February 19. Existing security protocols focus on securing the link between two machines to counteract eavesdropping. But making sure that a computer is connected to a legitimate access point in the first place is also important. If a hacker uses his computer as a fake access point and then relays the messages on to a real one, the information can be stolen covertly. The delayed password disclosure protocol counteracts this threat by allowing both parties to use a pre-arranged password or pin for authentication, but prevents this from being revealed during communications. Jakobsson adds that the scheme would not be noticed by users, as they are only notified when the wireless link seems suspicious. Computer code for the protocol will be released in the next couple of months and a version for mobile phones should also be ready by the end of 2005.
Source: <http://www.newscientist.com/article.ns?id=dn7037>
39. *February 18, K-Otik Security* — **WebCalendar "webcalendar_session" SQL injection vulnerability.** An SQL injection vulnerability was reported in WebCalendar, which may be exploited by attackers to execute arbitrary SQL commands. This flaw exists due to an input validation error in "login" when used in cookies. Update to WebCalendar version 0.9.5:
<http://www.k5n.us/webcalendar.php?topic=Download>
Source: <http://www.k-otik.com/english/advisories/2005/0184>
40. *February 18, SecurityTracker* — **Yahoo! Messenger lets remote users spoof filenames during file transfer.** A vulnerability was reported in Yahoo! Messenger in the file transfer feature. A remote user may be able to cause a target user to execute arbitrary code. Yahoo! Messenger does not properly display files with long filenames in the file transfer dialog windows. A remote user can send a specially crafted, long filename containing whitespace and two file extensions to spoof the filename. Update to version 6.0.0.1921, available at:
<http://messenger.yahoo.com/>
Source: <http://www.securitytracker.com/alerts/2005/Feb/1013237.html>
41. *February 18, Department of Homeland Security* — **Homeland Security launches regional technology integration initiative in Seattle.** The Department of Homeland Security on Friday, February 18, announced the addition of a new urban area to its Regional Technology Integration (RTI) initiative, which focuses on speeding the effective integration of innovative technologies and organizational concepts to the homeland security efforts of regional, state, and local jurisdictions. Through the program, managed by Homeland Security's Science & Technology directorate, four urban areas across the country have now been announced as the initial pilot locations for this program. The Seattle, Washington urban area joins Memphis, Tennessee; Anaheim, California; and Cincinnati, Ohio, as the pilot locations. These initial locations will provide the science and technology community with a realistic environment to test maturing hardware and concepts. The program will also provide information on how best to choose, deploy, and manage these technologies to strengthen the security posture of these and other communities. The goal of Homeland Security's Regional Technology Integration initiative is to facilitate the successful transfer and integration of existing and advanced

homeland security technology systems to local governments in order to improve their preparedness and response.

Source: <http://www.dhs.gov/dhspublic/display?content=4362>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis	
Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.	
US-CERT Operations Center Synopsis: On Tuesday, Microsoft published 13 security updates as part of their February security release. Eleven of the security bulletins affect Windows, and nine of the bulletins have been marked as "Critical." The US-CERT recommends ensuring that all Windows systems on your network have been patched for these vulnerabilities. Full information on the vulnerabilities, as well as links to the patches can be found at http://www.microsoft.com/security/default.msp	
Current Port Attacks	
Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 139 (netbios-ssn), 1025 (----), 1026 (----), 1027 (icq), 113 (auth), 80 (www), 53 (domain), 6346 (gnutella-svc) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
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

42. February 19, Georgia Tech Research News — Systems engineering approach offers paradigm for homeland security. Since the 2001 anthrax attacks, research has focused on developing improved sensors to detect potential chemical or biological terror agents. But these devices themselves cannot head off terrorist attacks, and while they should be part of an overall protection strategy, reliance on such technology can create a false sense of security, warns Art Janata, a Georgia Institute of Technology researcher. Janata says that a systems approach would include central command centers, response strategies tailored to the facility, protection of water and air circulation systems — and neutralizing and sterilizing chambers built into air-circulation systems to limit the spread of terror agents. “Almost every public building in the United States has a heating and air conditioning system that circulates the air,” Janata noted. “Not only does that refresh the air, but it also provides a vehicle for introducing both chemical and biological agents. The concept would be to insert into that system a sterilization chamber that would disable the biological agents and decompose the chemical agents.” A chamber exposing the air to ultraviolet light could inactivate most biological agents. And because of

their reactive nature, most chemical agents could be neutralized with a small number of chemical processes built into filtering systems.

Source: <http://gtresearchnews.gatech.edu/newsrelease/systemseng.htm>

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

General Sector

Nothing to report.

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

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

[Homeland Security Advisories and Information Bulletins](#) – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: <http://www.dhs.gov/dhspublic/display?theme=70>

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644.

Subscription and Distribution Information: Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644 for more information.

Contact DHS/IAIP

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.

DHS/IAIP Disclaimer

The DHS/IAIP 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.