



Department of Homeland Security Daily Open Source Infrastructure Report for 25 January 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

- Reuters reports utilities in five western U.S. states are in the process of setting up the Northern Tier Transmission Group, which is designed to facilitate coordination of big power lines in the area. (See item [1](#))
- The Washington Post reports as the number of armed pilots aboard U.S. jetliners has expanded, pilots complain about a lack of supervision and the difficulty in finding time to participate in training courses; federal security officials are launching a refresher training program next month to address this. (See item [14](#))

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. *January 23, Reuters* — **Five utilities form U.S. west transmission group.** Utilities in five western U.S. states are in the process of setting up the Northern Tier Transmission Group (NTTG), which is designed to facilitate coordination of big power lines in the area. The group is likely to announce plans for transmission line projects in the next half year, said Robert Kahn, spokesperson for the NTTG. The NTTG will not be an independent entity, so it will not serve as a regional transmission organization. The five utilities are PacifiCorp., Idaho Power, Northwestern Energy, Deseret Power Electric Cooperative, and the Utah Associated Municipal

Power Systems. The NTTG will strive to improve available transmission capacity and expedite planning for grid expansion and collaborating on control area operations. A plan to share control area operations has been developed by several NTTG members along with federal and state agencies including the Federal Energy Regulatory Commission.

Source: http://today.reuters.com/news/articleinvesting.aspx?view=CN&storyID=2007-01-23T204253Z_01_N23268033_RTRIDST_0_UTILITIES-NORTHWEST.XML&rpc=66&type=qcna

2. *January 23, Bloomberg* — **President Bush plans to double size of U.S. oil reserve by 2027.**

President George W. Bush plans to double the size of the country's emergency oil reserves to 1.5 billion barrels by 2027, Energy Secretary Samuel Bodman said. The government this spring will start buying 100,000 barrels of oil a day to fill the stockpile to its current capacity of 727 million barrels, Bodman said. Mark Routt of Energy Security Analysis Inc. said, "It's obviously a wise decision in terms of economic and political security." Secretary Bodman said, "Expanding the strategic petroleum reserve is a wise and prudent policy decision that will provide an additional layer of protection for our nation's energy security." The expanded reserve, stored in salt caverns along the U.S. Gulf Coast, would be equal to about 97 days of U.S. oil imports. It will cost about \$65 billion, including \$10 billion to build new storage facilities and \$55 billion for the extra crude, according to Energy Department spokesperson Craig Stevens. Said Jason Schenker, an economist at Wachovia Corp: "[The plan] would remove a significant amount of supply from the market. Refiners will have to spend more to get the available barrels."

Source: <http://www.bloomberg.com/apps/news?pid=20601103&sid=aG5IcyBW19.M&refer=us>

3. *January 23, Fulton Sun (MO)* — **Westminster students arrested for nuclear plant breach.**

Two Westminster College students are out on bond after allegedly breaching security last week at the Callaway Nuclear Power Plant in Missouri. Shawn K. Milligan and Corey A. Meyer were taken into custody at the plant by the Callaway County Sheriff's Department and charged with first-degree trespassing. Law enforcement officials would not divulge the reason the students gave for being at the facility, but did state that the incident is not considered to be connected with any terrorist act. Both the FBI and the U.S. Nuclear Regulatory Commission were contacted as part of standard procedure. The Callaway County Sheriff's Department handled the investigation. "They gave us a story, but that's something we can't discuss at this time," said Callaway County Sheriff Dennis Crane on Friday. "All we can say is that they were trespassing, they both bonded out on \$500 each, and that no other charges are expected." Crane also confirmed that a soft air pistol was found in the subjects' vehicle. AmerenUE security observed the two subjects drive into a fenced-in area of the plant and take pictures via a cell phone.

Source: <http://www.fultonsun.com/articles/2007/01/23/news/342news11.txt>

4. *January 23, Reuters* — **U.S. wind power seen growing by a quarter in 2007.**

Wind power generation in the United States will grow 26 percent in 2007, after increasing by 27 percent in 2006, the American Wind Energy Association (AWEA) said on Tuesday, January 23. In 2006, 2,454 megawatts of new wind generating capacity was installed, with \$4 billion invested, the AWEA said. Only natural gas generating plants accounted for more new power generation capacity last year. There are now about 11,604 MW of wind power generation capacity, up from 10,000 MW just four months ago. Texas installed 774 MW of new wind generation last

year, followed by Washington (428 MW), California (212 MW), New York (185 MW) and Minnesota (150 MW).

Source: http://today.reuters.co.uk/news/articlenews.aspx?type=scienceNews&storyID=2007-01-23T154627Z_01_N23243705_RTRIDST_0_SCIE_NCE-UTILITIES-WIND-DC.XML&WTmodLoc=SciHealth-C3-Science-6

5. *January 23, Government Executive* — **Lawmakers seek probe of DOE cyber-security programs.** The leaders the House Energy and Commerce Committee and two of its subcommittees are asking the Government Accountability Office for an investigation into the cyber-security programs at the Department of Energy (DOE). The letter from full committee Chairman John Dingell, (D-MI), ranking Republican Joe Barton of Texas and three subcommittee leaders notes that cyber-security weakness at DOE could allow "individuals or groups backed by nation-states" to access classified information. The department issued a report with new cyber-security rules after a 2005 attack removed detailed personnel information on 1,500 employees of the National Nuclear Security Administration. Last year, hundreds of classified documents from the Los Alamos National Laboratory were found in a worker's home during a drug raid.

Source: <http://www.govexec.com/dailyfed/0107/012307tdpm1.htm>

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

Chemical Industry and Hazardous Materials Sector

6. *January 24, Associated Press* — **Hazmat crews work to keep gas spill out of Bronx River.** A large gasoline spill at a service station in downtown White Plains, NY, caused severe traffic problems Wednesday, January 24, as hazardous materials crews scrambled to keep the gas from spreading in the Bronx River. A tanker truck was making a delivery at a gas station across from the federal courthouse when gas started spurting out of a tall venting pipe, said Deputy Police Chief Daniel Jackson. He said more than 1,000 gallons spilled onto the pavement and a roof of a nearby one-story building. Fire and hazardous waste crews placed booms in the Bronx River to contain the gasoline, but it was not immediately known how much got into the water. The roof and the surrounding pavement were foamed, and a strong odor of gasoline could be smelled as far away as the White Plains train station, about half mile away. It was not immediately clear if the spill was caused by operator or equipment error. Two nearby businesses, Efficiency Printing Company and Swift Electric Contracting Company, were kept closed because of the spill, but other businesses and the courthouse were not affected.

Source: http://ny.metro.us/metro/local/ap/NY_Gasoline_Spill.html

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

Defense Industrial Base Sector

7. *January 24, Federal Computer Week* — **DoD: Focused on data.** The Department of Defense (DoD) is concentrating on a data-centric strategy to move toward open systems based on service-oriented architecture (SOA) standards, John Grimes, assistant secretary of Defense for networks and information integration/chief information officer, said at a recent conference.

“Our focus is on data,” Grimes told the Network Centric Warfare conference in Washington, DC, on Wednesday, January 23. “As we go to SOA architecture, we keep the applications behind and share the data on the network, and it becomes very critical that data is understood by everyone.” DoD is using the Communities of Interest (COI) model as a basis for establishing data sharing, Grimes said. Next, DoD will work on a COI for strike capabilities, which would focus on building databases of target sets, Grimes said.

Source: <http://www.fcw.com/article97468-01-24-07-Web>

8. *January 23, Aviation Week* — **Anti-satellite test could lift small satellite, space spending.**

The United States should harden defenses around its space-based assets, experts say, and a recent Chinese anti-satellite (ASAT) attack test could lift the space segment of the defense industry and finally force a widespread debate over U.S. national security space policy, analysts suggest. "You'll need a balance of defensive and offensive capabilities," Heritage Foundation analyst Baker Spring said Monday, January 22, at a Capitol Hill forum hosted by the Marshall Institute's ongoing National Security Space project. "Ironically, the Chinese ASAT test should 'boost' the prospects for space-based missile defense," said Jeff Kueter, the institute's president. Peter Hays, a Science Applications International Corp. employee and senior policy analyst supporting the plans and programs division at the Defense Department's National Space Security Office, said that small, distributive space-based systems could particularly benefit compared with larger satellites — speeding up a shift that already started. The new attention could even re-energize the U.S. aerospace industry, he said.

Source: http://www.aviationweek.com/aw/generic/story.jsp?id=news/ASA_T01237.xml

9. *January 22, Reuters* — **Officials concerned about Chinese debris in space.** Trash from China's satellite-killing missile test has spread widely in space, creating a debris cloud that could jeopardize spy satellites and commercial imagery satellites in low orbits around Earth, U.S. officials said on Monday, January 22. Even the manned International Space Station is vulnerable to being hit by some of the thousands of pieces of trash created when China slammed a ground-based medium-range ballistic missile into an aging Chinese weather satellite about 537 miles above Earth on January 11, the officials said. "The test created a lot of debris. It definitely raises the possibility that something is going to be hit, including the space station," Peter Hays, a senior adviser to the Pentagon's National Security Space Office, told Reuters. Theresa Hitchens, who heads the non-profit Center for Defense Information, told a conference held by the George C. Marshall Institute that U.S. tracking data showed debris from the test had been seen from 266 miles to 1,875 miles above the Earth. "A huge number of satellites have been put in harm's way," she said, estimating that more than 120 satellites were orbiting in the area. It could take decades for debris from the Chinese weather satellite to fall out of orbit.

Source: http://today.reuters.com/news/articlenews.aspx?type=scienceNews&storyid=2007-01-23T001539Z_01_N22487285_RTRUKOC_0_US-CHINA-USA-SATELLITE.xml&src=rss&rpc=22

[[Return to top](#)]

Banking and Finance Sector

10.

January 24, Security Park (UK) — **Twenty percent of Trojans that infected computers during 2006 were designed to steal bank details.** Banker Trojans are Trojans designed to intercept access to bank Websites and steal the information entered in these pages, such as account numbers, credit card numbers, PINs or passwords. Then, they send this information to the creator of the Trojan so that he can use it for all types of crimes, from stealing money to identity theft. Banker Trojans represented twenty percent of the Trojans detected in 2006 by Panda ActiveScan. It was the most frequently detected category of Trojan. The Banker family, which accounted for 52.15 percent of the total, was the most frequently detected variant of banker Trojan. Banbra (39.08 percent), Goldun (6.32 percent), Bancos (2.36 percent), and Banking (0.09 percent) were the other most frequently detected Trojan families in 2006. At the moment, it could be said that there is no bank that offers online services whose users could not be affected by the banker Trojans in circulation. Many of these Trojans are variants of other Trojans that have emerged in the past.

Source: <http://www.securitypark.co.uk/article.asp?articleid=26381&CategoryID=1>

11. *January 23, Reuters* — **Coin shortage could turn pennies to nickels.** A potential shortage of coins in the United States could mean all those pennies in your piggy bank could be worth five times their current value soon, says an economist at the Federal Reserve Bank of Chicago. Sharply rising prices of metals such as copper and nickel have meant the face value of pennies and nickels are worth less than the material that they are made of, increasing the risk that speculators could melt the coins and sell them for a profit. Such a risk spurred the U.S. Mint last month to issue regulations limiting melting and exporting of the coins. But Francois Velde, senior economist at the Chicago Fed, says that prohibitions by the Mint would unlikely deter serious speculators who already have piled up the coinage. The best solution, Velde said, would be to "rebase" the penny by making it worth five cents rather than one cent. Doing so would increase the amount of five-cent coins in circulation and do away with the almost worthless one-cent coin. "These factors suggest that, sooner or later, the penny will join the farthing (one-quarter of a penny) and the hapenny (one-half of a penny) in coin museums," Velde said. Source: <http://www.ndtvprofit.com/homepage/news.asp?id=284684>

12. *January 23, Denver Post* — **Counterfeit money circulated at high school.** Two Columbine High School students have been arrested for their alleged roles in circulating counterfeit money at the south Jefferson County school in Colorado. The two male students — a 16-year-old and a 17-year-old — were charged Thursday, January 18, with fraud, said Jacki Kelley, spokesperson for the Jefferson County Sheriff's Office. The bills — in the denominations of \$1, \$2, \$5, \$10 and \$20 — surfaced last week, prompting school officials to notify parents by phone and e-mail. One boy allegedly created the bills on a home computer and printer and the other boy "was aware it happened and passed one of the bills," Kelley said. Kelley said some innocent students were approached and asked to make change for one of the fake bills, with the suspect receiving real bills in return. Authorities believe only "a handful" of counterfeit bills were circulated and the activity was limited within the high school. Source: http://www.denverpost.com/ci_5069903?source=rss

13. *January 23, CNET News* — **Start-up launches identity-theft search service.** A start-up has launched a service that lets people check whether their personal data is being traded online by criminals, but critics say it could be a boon for those same crooks. The service, dubbed StolenID Search, lets anyone with an Internet connection search a database of more than two

million credit card and Social Security numbers found in the recesses of the Internet, TrustedID, said Tuesday, January 23. Using StolenID Search is counterintuitive. Running a search requires the entry of the credit card or Social Security number that is to be checked against the database. This requires trust in TrustedID. Done right, experts see value in the new service. However, the way StolenID Search is set up now, it could play into the hands of criminals, they said. Assuming TrustedID can be trusted and its database is comprehensive, it can be valuable, said Gartner analyst Avivah Litan. StolenID Search could become a resource for criminals. For example, if a credit card number pops up as compromised on the Stolen ID Search Website, it will be of lesser value than when it doesn't.

Source: http://news.com.com/Start-up+launches+identity-theft+search+service/2100-7355_3-6152743.html?tag=cd.top

[[Return to top](#)]

Transportation and Border Security Sector

14. *January 24, Washington Post* — New demands for armed pilots. As the number of armed pilots aboard U.S. jetliners has steadily expanded in recent years, pilots and their labor groups complain about a lack of supervision and the difficulty in finding time to participate in training courses. Worried that pilots' handgun skills may be eroding, federal security officials are launching a refresher training program next month. Armed pilots must attend a two-day mandatory course at a training facility near Atlantic City three to five years after getting their guns. Some pilots have already taken prototype refresher courses that are being evaluated by authorities, said officials with the Federal Air Marshal Service, which runs the program. The controversial gun program, which started in 2003, was backed enthusiastically by pilots and their unions as a way to prevent terrorist hijackings after the September 11, 2001, attacks. When the program began, union officials said as many as 30,000 pilots would eventually carry firearms in cockpits. The number of armed pilots is well short of that number, but there are now more armed pilots than there are federal air marshals, according to sources familiar with the program.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/23/AR2007012301529.html>

15. *January 24, USA TODAY* — Valet parking landing at airports. Big airports are adding a service for time-pressed travelers: valet parking. More than a half dozen, including Miami, Indianapolis, Charlotte, Pittsburgh, Reagan Washington National, and Los Angeles, have added valet service in the last year. Cleveland, Atlanta and others are considering it. With a record number of passengers, airports are adding the service to gain revenue, differentiate themselves from competitors, and provide travelers with a time saving convenience. Valet parking is ideal for women traveling alone and for the elderly since they're met by attendants on arrival and can be watched into the terminal, says Greg Meyer, a spokesperson at Fort Lauderdale airport. Miami's valet attendants use wireless handheld devices that issue parking stubs and take digital photos of any existing damage to the car. Its valet lot also has a kiosk where customers can have the bar code on the parking stub scanned to calculate payment.

Source: http://www.usatoday.com/travel/flights/2007-01-24-valet-usat_x.htm

16.

January 24, Scotsman (Scotland) — **Edinburgh airport reopens after scare.** A bomb scare at Edinburgh Airport on Wednesday, January 24, caused massive disruption for thousands of travelers. The main terminal was evacuated shortly after midday when an unattended rucksack was spotted near the airport check-in desks. Airport staff contacted the police, who immediately cleared the building. Army bomb disposal experts were then called to carry out a controlled explosion on the suspect item. Once police deemed the incident a false alarm, the airport was reopened more than two hours after the alert was issued. Passengers were facing delays for the rest of the day as airlines struggled to return to their usual timetables. Several thousand passengers at the terminal, as well as airport workers, were evacuated to a nearby hotel as the incident unfolded.

Source: <http://news.scotsman.com/edinburgh.cfm?id=126732007>

17. *January 24, Reuters* — Jet hijacker wanted to fly to UK. A man armed with a pistol hijacked a Sudanese airliner on Wednesday, January 24, and tried to force it to fly to Britain, but it diverted to neighboring Chad where he was arrested and the passengers released unharmed. Chadian officials said the hijacker, a young Sudanese man, said he was trying to escape persecution in his own country. The Sudanese Air West Boeing 737 with 103 passengers and crew on board was on a domestic flight from Khartoum to el-Fasher in the conflict-torn Darfur region when it was hijacked 30 minutes after takeoff. "The hijacker was armed with a pistol and a knife. He demanded that the crew fly him to Great Britain but, due to lack of fuel, the plane had to land at N'Djamena," Chad's Infrastructure Minister Adoum Younousmi told Reuters. Relations between landlocked central African neighbors Chad and Sudan have been strained, with both countries accusing each other of supporting rebels seeking to topple their governments.

Source: <http://www.cnn.com/2007/WORLD/africa/01/24/sudan.hijack.reut/index.html>

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

Postal and Shipping Sector

18. *January 24, TCPalm (FL)* — Envelope containing mystery powder delivered to Florida home. An incorrectly addressed envelope believed to have some sort of powder inside of it was delivered to a home on Westmont Drive in St. Lucie County, FL, according to a sheriff's report. The homeowners reported the envelope, addressed to "Lifetime Guarantee" with the same address as their Fort Pierce home, felt as if "it contained unknown powdery substance" that could possibly be anthrax powder when they got their mail Monday evening, January 22, the report stated. They did not open it. Instead, they put it in a plastic bag and called authorities, who then sent the contents to a lab for testing. The envelope had Portugal mailing stamps on it, but did not have a return address. The homeowners did not know what Lifetime Guarantee was or who, if anyone, owned it.

Source: http://www.tcpalm.com/tcp/local_news/article/0.2545.TCP_1673_6_5301997.00.html

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

Agriculture Sector

19. *January 23, Brown University* — **Researchers find protein role in prion spread.** A single protein plays a major role in deadly prion diseases by smashing up clusters of these infectious proteins, creating the “seeds” that allow fatal brain illnesses to quickly spread, new Brown University research shows. The findings are exciting, researchers say, because they might reveal a way to control the spread of prions through drug intervention. If a drug could be made that inhibits this fragmentation process, it could substantially slow the spread of prions, which cause mad cow disease and scrapie in animals and, in rare cases, Creutzfeldt–Jacob disease and kuru in humans. The findings from build on the researchers groundbreaking work in 2005. That research showed that prions convert healthy protein into abnormal protein through an ultrafast process. This good–gone–bad conversion is one way that prions multiply and spread disease. But scientists believe that there is another crucial step in this propagation process — fragmentation of existing prion complexes. Once converted, the thinking goes, clusters of “bad” or infectious protein are smashed into smaller bits, a process that creates “seeds” so that prions multiply more quickly in the body.

Source: http://www.brown.edu/Administration/News_Bureau/2006-07/06-084.html

20. *January 09, World Organization for Animal Health* — **World Organization for Animal Health launches global animal health database.** The World Animal Health Information Database (WAHID) interface is now available on the World Organization for Animal Health (OIE) Web site and operational. This new extensive database is a milestone in OIE efforts to improve the transparency, efficiency and speed with which animal health information is disseminated throughout the world. Complementary to the on–line notification made by OIE Member Countries through the World Animal Health Information System (WAHIS) launched in April 2006, WAHID offers all available data on animal diseases, including zoonoses, per country, region, month and year. Among others, the database also compiles country animal population, exceptional epidemiological events maps, global animal diseases distribution maps or comparative disease status between two countries. The latter application can help define health hazards linked to the trade of live animals and animal products between countries.

WAHID: www.oie.int/wahid

Source: http://www.oie.int/eng/press/en_070109.htm

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

Food Sector

21. *January 24, Associated Press* — **Iowa company recalls hot dogs.** A slaughterhouse in Postville, IA, is recalling about 2,700 pounds of potentially underprocessed frankfurters shipped to the Northeast. Federal officials said Agriprocessors is accepting returns on the products shipped to stores in New Jersey, New York and Pennsylvania. No illnesses from these products have been reported. Company officials said an Agriprocessors employee discovered the problem and the company issued a voluntary recall.

Source: <http://www.kcci.com/news/10833644/detail.html>

22. *January 24, Agence France–Presse* — **U.S. pressure to ease Japan's beef import curbs.** The U.S. is putting fresh pressure on Japan to ease curbs on imports of U.S. beef, a half year after Tokyo lifted a total ban. In a letter to Japanese farm minister Toshikatsu Matsuoka, U.S. Trade Representative Susan Schwab and Agriculture Secretary Mike Johanns called on Japan to lift

the age limit in the regulations, the news agency Jiji Press reported Wednesday, January 24. On July 27 last year, the Japanese government resumed importing beef from cows 20 months or younger on condition that parts at higher risk of mad cow disease infection, including the brain and spinal cord, were removed. Japan, previously the top overseas market for U.S. beef, banned such imports in December 2003 after the discovery of the first U.S. case bovine spongiform encephalopathy (BSE). It partially lifted the import ban in December 2005 but reinstated all-out measures again a month later as prohibited cow parts were found in beef cargo from the U.S.

Source: http://news.yahoo.com/s/afp/20070124/pl_afp/healthjapanustra-demadcow_070124121816

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

Water Sector

23. *January 24, Reuters* — Corroded pipes and drinking water. Towns and cities across the U.S. spend more than \$50 billion each year cleaning water. More than 170,000 public water systems are at work to keep tap water meeting the standards of the Safe Drinking Water Act of 1974. But after the extensive purifying process, water travels through pipes laid under city streets 50, 60 or 100 years ago. Those pipes span almost one million miles. As the iron pipes corrode and break, not only does water escape, but also diseases get in, experts say. "Investigations conducted in the last five years suggest that a substantial proportion of waterborne disease outbreaks, both microbial and chemical, is attributable to problems within distribution systems," the National Research Council said. The amount of water lost is a sign the system is aging, experts say. In New York City, for example, the biggest leak in its system loses one billion gallons of water a month. "We estimate in the next 20 to 30 years water utilities will have to invest \$250 to \$350 billion just to replace the pipes that are in the ground today," said Jack Hossbuhr, executive director of the American Water Works Association, the industry's trade group.

Source: http://today.reuters.com/news/articlenews.aspx?type=scienceNews&storyID=2007-01-23T235437Z_01_N19331436_RTRUKOC_0_US-USA-WATER.xml&WTmodLoc=NewsHome-C3-scienceNews-2

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

Public Health Sector

24. *January 24, Reuters* — H5N1 bird flu confirmed in Hungary. The first outbreak of bird flu in the European Union (EU) this year was confirmed on Wednesday, January 24, after the EU Commission said the highly pathogenic H5N1 strain had been found in dead geese in Hungary. Tests were carried out for bird flu after an abnormally high mortality rate was reported in a flock of over 3,000 geese. All of the remaining flock were culled, the Commission said. It was the first finding of the disease in the 27-member bloc this year, but there have been fresh outbreaks of bird flu across Asia since the start of 2007. Five people have died of the H5N1 virus in Indonesia since January 1, while new cases in poultry have been reported in Japan, Thailand and Vietnam.

Source: <http://www.alertnet.org/thenews/newsdesk/L24581700.htm>

25. *January 24, Bangkok Post (Thailand)* — **Second Thai outbreak puts Asia on bird flu alert.** United Nations officials are urging Asian nations to be on alert for new bird flu outbreaks as Thailand reported a second H5N1 outbreak in the Northeast. 111 people were already being monitored for possible infection after an outbreak in ducks last week in Phitsanulok, authorities said. Now, the Livestock Department has confirmed a second outbreak in chickens in the Sri Chiang Mai district of Nong Khai, on the Mekong River across from Laos. Japan is also investigating a suspected outbreak at a poultry farm in the southwest. If confirmed, it would be the second outbreak this month of the H5N1 bird flu virus. The farm, which has about 50,000 birds, is situated in Hyuga in Miyazaki Prefecture, where 10 days ago the government confirmed an H5N1 outbreak.

Source: <http://www.bangkokpost.com/topstories.php?id=116255>

26. *January 24, Agence France–Presse* — **China says tainted blood stocks have led to hepatitis infections.** An unknown number of patients in China have contracted hepatitis C after a company distributed tainted blood in one of its immune system–boosting antibody products, the government has said. Sales of the company's products have been halted while patients who may have used the tainted blood are being tracked down, according to a statement from the Ministry of Health and the State Food and Drug Administration Wednesday, January 24. The statement said Guangdong Bioeye Pharmaceutical had acted illegally in its production of immunoglobulin, an intravenous drug for treating immune system deficiencies and viral infections. The statement said the company, in the southern province of Guangdong, could not produce a complete set of production and inspection records for the products.

Source: http://news.yahoo.com/s/afp/20070124/hl_afp/healthchinadisea_se_070124102222

27. *January 24, Reuters* — **Two flu shots needed to protect young children.** Infants and toddlers given two doses of the influenza vaccine are less likely to contract flu, pneumonia and influenza–like illnesses, but one dose does not appear to have any effect. Mandy Allison, of the University of Utah, Salt Lake City, and colleagues examined the effectiveness of the currently recommended two–dose influenza vaccine for young children, as well as the effect of one dose of the vaccine, in preventing visits to the doctor for influenza–like illness. They analyzed data for 5193 healthy children between the ages of six and 21 months who were seen at five Denver pediatric practices during the 2003–2004 flu season. The kids were defined as being partially vaccinated if they had one shot more than 14 days before the first influenza–like illness visit, and fully vaccinated if they had the full two shots more than 14 days before the first visit. Overall, 28 percent of the children were seen for influenza–like illness and five percent had a visit for pneumonia/influenza. Full vaccination was 69 percent effective in preventing office visits for influenza–like illness and 87 percent effective in preventing office visits for pneumonia/influenza. Partially vaccinated children were just as likely to be seen for influenza–like illness as were unvaccinated children.

Source: http://today.reuters.com/news/articlenews.aspx?type=healthNews&storyID=2007-01-24T002020Z_01_KIM401172_RTRUKOC_0_US-TWO-FLU-SHOTS.xml&WTmodLoc=NewsHome-C3-healthNews-3

[[Return to top](#)]

Government Sector

28. *January 24, Inside Bay Area (CA)* — **Police destroy suspicious device at Ohlone College.** A suspicious device found at Ohlone College, in Fremont, CA, was destroyed by the county bomb squad Monday afternoon, January 22, but authorities have not yet been able to determine exactly what it was, police said. The device, which looked a like soup can wrapped in duct tape with an M-80 firework sticking out of it, was spotted about 1:15 p.m. PST in the south parking lot of the campus, Fremont police Sgt. Chris Mazzone said. Police cordoned off the area and called the bomb squad, which eventually used a water cannon to destroy the device, the sergeant said. When it blew up, there was a brief cloud of orange mist and some dried residue left behind. Police collected samples of it and sent it to a lab for analysis, Mazzone said. Source: http://www.insidebayarea.com/argus/localnews/ci_5074282
29. *January 24, KTAR (AZ)* — **Legislators return to Phoenix Capitol after bomb scare.** Two unexpected packages that arrived at the Arizona House of Representatives triggered an evacuation shortly after noon on Wednesday, January 24, and the arrival of the bomb squad. One package was addressed to lawmaker Kyrsten Sinema, who has been the target of recent e-mails advocating sexual violence over her proposal to declare groups like the Minutemen as domestic terrorists. Source: <http://www.620ktar.com/?nid=6&sid=350422>

[[Return to top](#)]

Emergency Services Sector

30. *January 24, Evening Telegram (NY)* — **High school students complete firefighter training course.** The Frankfort, NY, Fire Department has some new graduates who have taken the first step to becoming firefighters. On Tuesday, January 23, four Frankfort-Schuyler Central School seniors graduated from the school's firefighter program having completed the New York State Firefighter 1 course. The four each received school credit for the elective class. As part of the program, the students volunteered 120 hours of community service and completed 78 hours of training. Fire Chief Charles Conigliaro said the course is basic firefighter's training and is the first step toward being a firefighter and that all four will continue their education in the program this spring. Conigliaro said the five-year-old program helps the department seek volunteers and that most of the graduates go to college and return to the department in the summer to help out. Source: http://www.herkimertelegram.com/articles/2007/01/24/news/new_s03.txt
31. *January 24, Baytown Sun (TX)* — **Officials pleased with mock disaster drill.** The town of Baytown, TX, participated in a statewide drill Tuesday, January 23. Before noon, Baytown had already endured a fake explosion at industrial docks on the Houston ship channel, a mock explosion of a pipeline corridor running by the San Jacinto Methodist Hospital and a robbery at the Community Resource Credit Union. By noon, the drill was completed and participants from the Baytown Police Department, Baytown Fire Department, Emergency Medical Services, Emergency Operations Center, Community Resource Credit Union, San Jacinto hospital and Exxon Mobil were ready with their evaluations. All three simulated events provided

participating companies and individuals the chance to evaluate their personal strengths and weaknesses when responding to a disaster. The main points of improvement listed from most participants were the need for increased communication and the additional or improved equipment that would make that possible.

Source: http://stories.baytownsun.com/story.lasso?ewcd=8bce73748d1b3_f17

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

Information Technology and Telecommunications Sector

32. *January 24, IDG News Service* — Apple patches security flaw in QuickTime. Apple Inc. has patched a vulnerability in its QuickTime media player that could give a hacker control over a computer. The problem concerns a buffer overflow that can occur when QuickTime processes a Real Time Streaming Protocol Uniform Resource Locator (RTSP URL), which directs the player to a streaming file and allows a user to play and pause it. A hacker could create a malicious RTSP URL embedded in a Webpage that would open a door for other harmful code to run on a machine, Apple said. The patch comes more than three weeks after researchers who are part of the Month of Apple Bugs project published exploit code.

QuickTime patch: <http://www.apple.com/support/downloads/>

Source: http://www.infoworld.com/article/07/01/24/HNquicktimepatch_1.html

33. *January 24, Sophos* — Storm worm turns to love in major new attack. Sophos is warning of a major new malicious attack occurring against Internet users. New variants of the Dorf malware family (earlier incarnations of which purported to be breaking news of deaths caused by European storms) are now using disguises associated with love and greeting cards. Subject lines used in the spam campaign are many and varied. Some of them include "You're so Far Away," "I Dream of you," "Old Together," "Dream Date Coupon," "Together You and I," "A Bouquet of Love," "So in Love," "Cuddle Up," and "Vacation Love." Attached to the e-mails are files called flash postcard.exe or greetingcard.exe, which contain the worm. Opening the attached files on a PC activates the worm, which then sends itself to other e-mail addresses found on the now infected computer. Sophos analysts believe that the worm code is designed to attempt to download further malicious code from the Internet designed to take over the PC, convert it into part of a zombie network, and use it to send spam on behalf of hacking gangs.

Source: http://www.sophos.com/pressoffice/news/articles/2007/01/dorf_love.html

34. *January 24, Sophos* — Couple sued for sending five million spam cell phone messages. Sophos has warned of the rising nuisance of spam sent to mobile phones as two people from Florida have been charged with flooding cell phones with spam messages advertising time shares. Illinois Attorney General Lisa Madigan has filed a suit against Neela Pundit and Charles Rossop for sending five million unsolicited text messages to cell phone owners across the country. More than 200 consumers complained in Illinois alone after receiving the advertisements in October and November 2006 which read: "We have someone interested in buying or renting your Time Share." The advertisement encouraged recipients to visit two Internet Websites.

Source: http://www.sophos.com/pressoffice/news/articles/2007/01/smss_pam.html

35. *January 23, Information Week* — **One hacker kit accounts for 71 percent of attacks.** A multi-exploit hack pack was responsible for nearly three-fourths of all Web-based attacks during December, a security company said Tuesday, January 23. Tagged with the moniker "Q406 Roll-up," the attack kit was behind 70.9 percent of last month's attacks, reported Atlanta, GA-based Exploit Prevention Labs. Up to a dozen different exploits make up the kit, which includes several exploits derived from the proof-of-concept code that researcher HD Moore published in July 2006 during his "Month of Browser Bugs" project. It's difficult to tell the exact number of exploits in the package, said Exploit Prevention's chief technology officer, Roger Thompson, because the kit is heavily encrypted. The most common exploits found in the kit are setSlice, VML, XML, and (IE COM) Createcomobject Code. "The dominance of this package reinforces the fact that the development and release of exploits frequently parallels legitimate software businesses," Thompson said in a statement.

Source: <http://www.informationweek.com/news/showArticle.jhtml?articleID=196902970>

36. *January 23, eWeek* — **Compatibility concerns hinder Vista upgrades.** Microsoft's new operating system may be the most eagerly anticipated release of the past 10 years, but concerns over compatibility, bugs and security are keeping many IT professionals from doing so soon, according to the survey released Tuesday, January 23, by Cambridge, MA-based Bit9, a provider of desktop lockdown solutions. Only 68 percent of IT pros reported that they'd be upgrading to Vista in 2007, though very few had made immediate plans. Of those who had expressed their intention to shift to the new operating system, 58 percent said they'd be waiting six months to one year after the launch to do so, while but 10 percent planned to roll out the upgrade in the next six months.

Research Brief (registration required):

http://www.bit9.com/files/Bit9_Vista_Survey_Research_Brief_v.f.pdf

Source: <http://www.eweek.com/article2/0,1895,2086703,00.asp>

37. *January 23, IDG News Service* — **Google.de domain gets kidnapped.** Visitors to the German Website of Google were met with a strange sight early Tuesday morning, January 23: Gone was the Google logo, replaced by the name of a local Internet service provider with the message that no content was available for the domain. The Internet address of google.de and the page name were transferred to the new ISP, Goneo Internet GmbH, in a domain name grab that has confused Google users and infuriated company officials. Not all of Google's German Websites were affected by the domain grab, and those that were got restored within approximately two hours. In Google's case, two key security measures to prevent domain hijacking failed, a situation that could lead to changes in German domain name regulations, according to German domain registry Denic eG.

Source: http://www.infoworld.com/article/07/01/23/HNgooglegermany_1.html

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	The top 10 Target Ports are temporarily unavailable. We apologize for the inconvenience. 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

Nothing to report.

[[Return to top](#)]

General Sector

Nothing to report.

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

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

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to 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.