



Department of Homeland Security Daily Open Source Infrastructure Report for 15 May 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

- The Associated Press reports the Empress of the North — a cruise ship that ran aground at the southern end of Icy Strait, off the Alaskan coast — was moving under Coast Guard escort after its passengers had been evacuated. (See item [17](#))
- The Department of Homeland Security will soon begin conducting multiple projects in the Port of Tacoma, to evaluate technology and concepts of operations for radiation detection that will scan cargo at various points in transfer from ship to rail. (See item [19](#))
- WCBD reports Karen Wyndham, of Cottageville, South Carolina, was charged with tampering with consumer products after placing rodent poison into three previously sealed packages of ground beef, and then putting the tainted meats in the meat display of a Super K-Mart store. (See item [27](#))

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. *May 12, Washington Post* — **Venezuelan oil losing share of key U.S. market.** When the state oil company recently took over the last privately run oil fields in Venezuela, President Hugo Chávez declared it a victory against Washington and a giant leap toward a new energy policy

that would diversify the market for Venezuelan crude to include rising powers like China. Chávez often warns that he'll shut off the oil spigot to the U.S. if the Bush administration invades Venezuela or hatches an assassination plot against him. But new study of trade and oil consumption data shows that Venezuela appears ever more dependent on selling its oil to the U.S. And U.S. government energy trade data show the United States is slightly less dependent on Venezuela, which at one time challenged Canada, Mexico and Saudi Arabia as the number one provider of foreign oil but now tussles with up-and-coming Nigeria for the fourth spot. "Venezuela is losing its privileged position," said Alberto Quiros, former executive at Royal Dutch/Shell and at Venezuela's state oil company, *Petróleos de Venezuela S.A.* "The United States' needs have increased and Venezuela's ability to supply has decreased."

Source: http://www.washingtonpost.com/wp-dyn/content/article/2007/05/11/AR2007051102166_pf.html

2. *May 11, Associated Press* — **Natural gas terminals raise safety concerns.** While the energy industry regards liquefied natural gas (LNG) as a vital to keeping up with the demand for natural gas, proposals to build terminals are raising environmental and safety concerns. Energy companies have proposed 35 new U.S. terminals in ten states and five coastal offshore areas. Eighteen terminals have been approved by the Federal Energy Regulatory Commission. Along with LNG plant construction comes fears of accidents or terrorist attack. Leaks at terminals and on tankers that could allow the liquid to heat up quickly and return to its flammable gas form. The biggest concern centers on safety. In 2004, an explosion at an LNG plant in Algeria killed 30 people. The worst accident on record happened in 1944, at a Cleveland LNG plant that burned and killed 128 people after a tank leaked LNG into the sewer system where it became a flammable vapor and exploded. A congressional study recently said fire from a terrorist attack on an LNG tanker could cause the gas to ignite so fiercely that it would burn people several miles away. The Government Accountability Office said most experts believe intense heat — not explosions — would likely be the biggest threat to the public.

Source: <http://www.canada.com/calgaryherald/news/calgarybusiness/story.html?id=a02bedf3-e42b-4465-bb9e-1a602926829a>

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

Chemical Industry and Hazardous Materials Sector

3. *May 14, WYFF4 (SC)* — **Roads closed briefly after chlorine leak.** Two Spartanburg County, SC, roads reopened Sunday night, May 13, after firefighters closed them for more than an hour because of a chlorine gas leak. The Greer Fire Department said the leak came from a one-ton cylinder at the Maple Creek Waste Treatment Plant. Firefighters shut down part of Highway 80 and Gilliam Road while they shut off the valves to the cylinder and allowed the gas to dissipate. Source: <http://www.wyff4.com/news/13311969/detail.html?rss=gs&psp=news>
4. *May 13, Associated Press* — **Ammonia leak forces evacuation of four-square-mile area in Indiana.** Anhydrous ammonia that leaked from a farm tank forced the evacuation of a four-square-mile area in northeastern Indiana and left a motorist and four firefighters with minor facial burns, officials said. All five people were treated at the scene and refused hospitalization after a hose detached from a pull-behind ammonia tank Friday, May 11, said LaOtto fire chief Jim Molargik. "Something mechanical broke," he said. Authorities evacuated

residents within a four-square-mile area around the leaking tank due to concerns that shifting winds could overwhelm residents before they could flee from the toxic gas. Officials said it was unclear how many people were evacuated from the town 15 miles north of Fort Wayne. The leak shut down Old State Road 3, LaOtto's main road, for nearly two hours.

Source: <http://www.southbendtribune.com/apps/pbcs.dll/article?AID=/20070513/News01/70513035>

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

Defense Industrial Base Sector

5. *May 14, Government Accountability Office* — **GAO-07-733: DoD Business Systems Modernization: Progress Continues to Be Made in Establishing Corporate Management Controls, but Further Steps Are Needed (Report)**. In 1995, the Government Accountability Office (GAO) first designated the Department of Defense's (DoD) business systems modernization program as "high risk," and GAO continues to do so today. To assist in addressing this high-risk area, the Fiscal Year 2005 National Defense Authorization Act contains provisions that are consistent with prior GAO recommendations. Further, the act requires the department to submit annual reports to its congressional committees on its compliance with these provisions and it directs GAO to review each report. In response, GAO assessed DoD's actions to address (1) requirements in the act and (2) GAO's recommendations that it reported as open in its prior annual report under the act. In doing so, GAO reviewed documentation and interviewed officials relative to the act and related guidance. GAO is recommending that future DoD annual reports include an assessment by its independent verification and validation agent of the quality of the department's federated family of architectures, including the associated transition plan(s). In written comments, DoD agreed with GAO's recommendation.

Highlights: <http://www.gao.gov/highlights/d07733high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-733>

6. *May 11, Government Accountability Office* — **GAO-07-538: Business Systems Modernization: DoD Needs to Fully Define Policies and Procedures for Institutionally Managing Investments (Report)**. In 1995, the Government Accountability Office (GAO) first designated the Department of Defense's (DoD) business systems modernization program as "high-risk," and continues to do so today. In 2004, Congress passed legislation reflecting prior GAO recommendations for DoD to adopt a corporate approach to information technology (IT) business system investment management. To support GAO's legislative mandate to review DoD's efforts, GAO assessed whether the department's corporate investment management approach comports with relevant federal guidance. In doing so, GAO applied its IT Investment Management framework and associated methodology, focusing on the framework's stages related to the investment management provisions of the Clinger-Cohen Act of 1996. GAO recommends that DoD fully define the project and portfolio management policies and procedures discussed in GAO's framework. DoD agreed with GAO's overall conclusions and partially agreed with five of GAO's recommendations. However, DoD disagreed with the remaining four recommendations, stating that the department is, among other things, already meeting the intent of these recommendations. GAO does not agree; its recommendations focus on fully defining policies and procedures that satisfy key practices in its framework.

Highlights: <http://www.gao.gov/highlights/d07538high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-538>

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

Banking and Finance Sector

7. *May 14, VNUNet* — **U.S. brands milked for phishing e-mails.** Household U.S. brands are still routinely used in phishing attacks to draw in unsuspecting users, according to RSA's Monthly Online Fraud Report. It found that the share of U.S. brands made up 73 percent of all entities being phished in April. "As in February and March, UK institutions remained in the number two spot, with 10 percent of the phished entities," the report said. However, the number of institutions coming under attack decreased in April, following an increase in March. There was also drop in the number of attacks hosted in the U.S. Hong Kong moved up to second position from third spot last month, with 15 percent of phishing attacks hosted in the country. South Korea and China also joined the top of the list of countries hosting attacks, as Russia was pushed out of the top five.
Source: <http://www.vnunet.com/vnunet/news/2189751/brands-milked-phishing-emails>
8. *May 14, The State (SC)* — **Drug bust uncovers fake ID operation.** The Lexington County, SC, seizure in January of 11 pounds of cocaine from illegal Mexican immigrants has led to the discovery of a fake Social Security card and identity theft operation, authorities say. About 20 members and associates of a Lexington County Mexican family, many illegally in the United States, have been linked so far to the fake Social Security numbers operation. The case is believed to be the biggest S.C. investigation to combine drug smuggling, illegal immigrants from Mexico and fake identities. It also is an example of how easy it is to use fake and counterfeit Social Security cards and numbers in the United States and the Columbia area, said U.S. Attorney Reggie Lloyd. The suspects are believed to have made more than \$1 million. The investigation also involves an unspecified "financial investigation," according to federal records and Drug Enforcement Administration Agent Todd Briggs. Indictments in the current case allege illegal immigrants used fake Social Security numbers and wage statements in a variety of ways. The immigrants also used the numbers to sign up for power with S.C. Electric & Gas Co., register with the S.C. Employment Security Commission, apply for leases and buy a Cadillac.
Source: <http://www.thestate.com/426/story/63354.html>
9. *May 14, Security Focus* — **Pirate Bay breach leaks database.** The Pirate Bay announced on Friday, May 11, that an attacker exploited a security hole in the peer-to-peer directory's blogging software to copy a list of the site's usernames and passwords. The site, which allows visitors to search for files offered by members via a BitTorrent peer-to-peer network, currently has 1.4 million members that offer for download -- or "seed" -- various videos, audio and game files, many of them pirated. While site operator "brokep" warned users to change their passwords, he also said that decrypting the password file will likely take a long time. The Pirate Bay is a well-known BitTorrent tracking site started by a Swedish anti-copyright organization in 2003, but became managed separately by "dedicated individuals" in October 2004. Swedish authorities raided the organization's servers, based in Stockholm, in May 2006, but the torrent tracker was back online three days later.

Source: <http://www.securityfocus.com/brief/499>

10. *May 11, Guardian (UK)* — Warning on terrorist charity links. Forty-eight "suspicious activity" reports about links between charities and terrorist financing were filed last year by banks and other financial institutions, according to a UK Home Office review published Thursday, May 10. It says that Serious Organized Crime Agency reports show that while terrorist exploitation of charities has proved rare, it remains a risk. A consultation paper by the Home Office and the Treasury proposes that the Charity Commission works far more closely with police and security services to crack down on charities which are used as a front for terrorist fundraising. The paper also recommends that the commission has more access to classified intelligence information to identify phony charities. The review says that 34 of the 48 reports proved substantive enough to warrant further investigation.

Source: <http://www.guardian.co.uk/terrorism/story/0,,2077207,00.html>

11. *May 10, Reuters* — U.S. banks seek to reduce cash, suspicious reports. Small U.S. banks face the same costly requirements as big banks to meet regulations aimed at rooting out drug trafficking, money laundering and terrorist financing, an industry group told lawmakers on Thursday, May 10. U.S. law enforcement officials said financial institutions filed 17.6 million cash transaction reports, suspicious activity reports and others under the Bank Secrecy Act in fiscal 2006. Small banks and credit unions have complained that the cost, time and staff needed to comply considerably drains their budgets. "This takes resources from other areas where the money could be better used," Carolyn Mroz of Bay-Vanguard Federal Savings Bank said to the House Financial Services panel hearing. The data is vital to the Financial Crimes Enforcement Network (FinCEN) to combat and prosecute terrorist financing activities. The goal of the hearing was to examine the costs and benefits of the reports — which have steadily increased from 15.6 million in fiscal 2005 — to see if legislation is needed to alter the amount of reports. William Baity of FinCEN said it is trying to maintain the balance of the needs of law enforcement and the costs for financial institutions, which also include casinos and card clubs, and money service businesses.

Source: http://www.reuters.com/article/governmentFilingsNews/idUSN09_27199620070510

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

Transportation and Border Security Sector

12. *May 14, Associated Press* — Amtrak train evacuated after bomb threat. An Amtrak train carrying nearly 140 passengers was evacuated near Denver after a passenger threatened the crew and others onboard, claiming he had a weapon and bomb, an Amtrak spokesperson said early Monday, May 14. Police met the California Zephyr train about 22 miles west of Denver late Sunday after the crew alerted authorities about the unidentified passenger's threats, Amtrak spokesperson Karina Romero said. Authorities detained the man for questioning and did a sweep of the baggage car and the passenger car where he was sitting. The man was carrying a knife, and a bomb-sniffing dog focused on his bag, Romero said. "There was something that was in that bag that made the dog stop," Romero said, declining to elaborate. Passengers were evacuated and transported by bus back to Denver, Romero said.

Source: http://hosted.ap.org/dynamic/stories/T/TRAIN_EVACUATION?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

13. *May 14, Reuters* — **U.S. airlines risk ballooning frequent-flyer payout.** Frequent flyer reward schemes have ballooned over the years and carriers now risk paying a high price for the glut. Airlines have awarded more than 19 trillion frequent flyer miles over the past 25 years — roughly equivalent to circling the globe 760 million times — and more than 14 trillion of those miles are unredeemed. The rate of awards is increasing annually, according to frequent flyer site WebFlyer. AMR Corp., parent of American Airlines, which operates the world's largest frequent-flyer program, carried a \$1.6 billion liability on its books at the end of 2006, about \$100 million more than a year earlier and up from \$976 million in 2000. With planes fuller than ever, granting free trips could displace paying passengers, while unsettled U.S. consumers may be ready to cash in those miles to save money as the economy shows signs of slowing. After the September 11, 2001, attacks sent the airline industry into a decline, carriers began awarding more and more frequent-flyer miles in order to encourage customers to fly. In addition, credit cards and other award schemes have allowed consumers to accumulate miles by buying anything from sliced bread to gasoline.

Source: http://www.usatoday.com/travel/flights/2007-05-14-frequent-flyers_N.htm

14. *May 14, Town Talk (LA)* — **Prank call leads to arrest after Louisiana airport shut down.** A prank call that shut down Alexandria International Airport Saturday, May 12, led to the caller's arrest, a Rapides Parish, LA, Sheriff's Office spokesperson reported Monday, May 14. Wardell Winbush, 58, of 4003 Clinton St., Alexandria, was arrested and charged with one count terrorizing (making a false statement), according to Sgt. Tracy Bellino with the Rapides Parish Sheriff's Office. Bellino said a call was received 5 p.m. CDT Saturday at the sheriff's office warning about a woman who would try to board a plane with a firearm and discharge it while in flight. Rapides Parish Sheriff's security officers on duty at the airport as well as federal authorities were alerted immediately and shut down all air traffic from leaving or arriving at the airpark, Bellino said. Passengers were removed from a plane and Transportation Security Administration officers searched the passengers and luggage but no weapon was located, Bellino said. The flight, Continental 3230 to Dallas, was delayed about 90 minutes before it was allowed to leave after being searched again.

Source: <http://www.thetowntalk.com/apps/pbcs.dll/article?AID=/20070513/NEWS01/70513006/1002>

15. *May 14, Government Technology* — **Governor Rendell announces federal grant to enhance port security.** Governor Edward G. Rendell said Pennsylvania's ports in Erie, Philadelphia, and Pittsburgh will be more secure now that the state and private entities that operate them are receiving \$8.6 million worth of grants. The grants will be awarded through the U.S. Department of Homeland Security's port security grant program. A grant to the Pennsylvania State Police is the only one awarded to a state agency. Other agencies receiving federal grants include the City of Pittsburgh, Erie–Western Pennsylvania Port Authority, and the Philadelphia Regional Port Authority. A terrorist attack on the Port of Philadelphia, with its extensive petrochemical refining capabilities, cargo facilities and military presence, could result in the loss of lives and critical infrastructure," State Police Commissioner Jeffrey B. Miller said.

Source: <http://www.govtech.net/news/news.php?id=105439>

16. *May 14, AM New York* — **National Guard patrolling PATH stations.** National Guard troops began patrolling 13 Port Authority Trans–Hudson (PATH) stations in New Jersey and New

York on Monday, May 14. The patrols are similar to ones at New York's Penn Station and Grand Central Station and were not in response to a threat. The deployment is designed to bolster existing security by adding more manpower at mass transit stations, the Port Authority of New York and New Jersey said. The pilot program, which is costing \$200,000 a month, will deploy up to 40 National Guard troops. The transit system is already patrolled by Port Authority police, including K-9 detection and special operations units.

Source: <http://www.amny.com/news/local/wire/newjersey/ny-bc-nj--path-nationalguar0514may14.0.2583610.story?coll=ny-mets-print>

17. *May 14, Associated Press* — **Cruise ship aground in Southeastern Alaska.** A cruise ship that ran aground off the Alaska coast was moving under Coast Guard escort after its passengers were evacuated. Chief Petty Officer Barry Lane said all passengers had been evacuated from the Empress of the North and the vessel was moving again with 29 crew members on board by 7 a.m. Alaska time. The Empress of the North, carrying 281 passengers and crew, sent out an emergency radio message at 12:35 a.m. local time and the Coast Guard responded with an aircraft and helicopter. The vessel took on water and was listing six degrees at the southern end of Icy Strait, about 15 miles southwest of Juneau, said Petty Officer Christopher D. McLaughlin at the Coast Guard base in Kodiak. Over the following hours, passengers were transferred from the Empress of the North to fishing vessels and other cruise ships that were in the area. It wasn't immediately clear why the cruise ship ran around, McLaughlin said. Seas were calm. The Empress of the North is operated by Majestic America Line of Seattle.

Source: <http://www.adn.com/front/story/8883718p-8784093c.html>

18. *May 11, Reuters* — **Smart cameras to tackle abandoned luggage alarms.** A suitcase lies abandoned in a busy airport terminal. Was it planted by a bomber, or carelessly left for a couple of minutes while the owner went to buy coffee? One of the commonest headaches facing security staff may soon be remedied with the help of "intelligent security cameras" developed by European scientists. A newly concluded research project relies on formulae known as algorithms to enable computers to analyze video images and spot potential threats, from abandoned baggage to people loitering suspiciously. For security staff at airports or railway stations, often monitoring images from dozens of surveillance cameras at once, the new technology offers the promise of picking out dangers that might otherwise be missed. "The idea is to automatically analyze and intelligently filter all of that video, but also to add a next level of intelligence," said James Ferryman, a specialist in 'computational vision' at the University of Reading in England.

Source: <http://uk.reuters.com/article/technologyNews/idUKL2016544320.070511>

19. *May 11, Department of Homeland Security* — **DHS establishes rail test center for radiation detection.** The Department of Homeland Security (DHS) will soon begin conducting multiple projects in the Port of Tacoma, WA, to evaluate technology and concepts of operations for radiation detection that will scan cargo at various points in transfer from ship to rail. By establishing a Rail Test Center (RTC) at the port, DHS will identify and evaluate radiological and nuclear detection solutions for intermodal rail port facilities that can be used across the country. Projects being considered for further evaluation at the RTC include scanning cargo on the dock, during transport to the rail yard, entering the rail yard, in the container storage stack, during train assembly, and as the train leaves the port. The Port of Tacoma is a publicly owned facility and the seventh largest container port in North America --- handling more than 70

percent of its total import cargo volume by rail at multiple intermodal rail terminals. DHS's Domestic Nuclear Detection Office is a jointly staffed, national office established to improve the nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the nation, and to further enhance this capability over time.

Source: http://www.dhs.gov/xnews/releases/pr_1178919294310.shtm

20. *May 10, Transportation Security Administration* — **TSA officer spots passenger in fake military uniform at Florida airport.** A Transportation Security Administration (TSA) behavior detection team at a Florida airport helped catch a passenger impersonating a member of the military on Thursday, May 10, as he went through the security checkpoint. The passenger, who was en route to New York's John F. Kennedy International Airport, exhibited suspicious behavior that caught the attention of officers. In addition, he was in a military uniform but had long hair, which is not consistent with military regulations, and had conflicting rank insignias on the uniform. When officers asked for his military identification, the passenger said he had none. He was then questioned about the irregularities of his uniform. The passenger first claimed that the uniform was his brother's, and later, that it was his nephew's. TSA contacted law enforcement partners at the airport who interviewed the passenger. Fernando Montas of Ocala, FL. He was arrested on a state charge of impersonating a U.S. soldier. Behavior detection officers are trained to focus on behavior and not physical characteristics as part of TSA's Screening of Passengers by Observation Techniques, or SPOT program.
Source: http://www.tsa.gov/press/happenings/florida_uniform.shtm

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

21. *May 12, Associated Press* — **Deadly fish virus found in inland Wisconsin waters.** A deadly fish virus has been found in the Lake Winnebago chain of lakes — the first such infection confirmed in inland Wisconsin waters, the state Department of Natural Resources (DNR) said Saturday, May 12. Two freshwater drum fish, or sheepshead, from Little Lake Butte des Morts preliminarily tested positive for viral hemorrhagic septicemia (VHS), which causes anemia and hemorrhaging in fish. Other freshwater drum samples taken from Lake Winnebago, home to a large population of sturgeon, also appear to have the virus, the DNR said. State fish experts suspect the disease is also in Lake Michigan, Lake Superior and the Mississippi River.
Source: <http://www.mlive.com/sportsflash/michigan/index.ssf?/base/sports-23/1179010441187580.xml&storylist=michigansports>
22. *May 12, Daily Advertiser (LA)* — **White spot disease confirmed in crawfish pond.** The National Veterinary Service Laboratory has confirmed the presence of white spot disease in a quarantined crawfish pond in St. Martin Parish, LA. The pond was quarantined in late April

after state Department of Agriculture and Forestry officials and aquaculture specialists from Louisiana State University suspected the disease was causing crawfish in the pond to die. The disease can severely reduce production and has caused mortality rates of 100 percent in farmed shrimp.

Source: <http://www.theadvertiser.com/apps/pbcs.dll/article?AID=/20070512/NEWS01/70512012/1002>

23. *May 11, Messenger (GA)* — **Mystery pig disease strikes Georgia.** Over 3000 pigs have dropped dead over the last three weeks in the provinces of Guria and Samegrelo in western Georgia. Rustavi 2 reports that the 3000 dead pigs have been dumped into local rivers by farmers. The TV station also reports that infected meat is being sold at markets in Samegrelo. Head of the National Service of Food Safety, Veterinary and Plant Protection Department, Levan Orkoshneli told The Messenger on May 10, "Information was spread erroneously: the widespread disease is not a 'pig plague'." He explained that they have not identified exactly what the disease is but they suspect it is a particular kind of virus that attacks a pig's immune system making the animal vulnerable to disease. Orkoshneli explained that the virus spread quickly because of a lack of sanitary and hygienic conditions. He says this kind of virus is common in Europe. Guram, a pig farmer from the Lanchkhuti district of Guria told The Messenger that the first case of the disease appeared not a few weeks ago on his farm, but a few months ago. "The disease first appeared on my farm in February. In February, 155 of my pigs died."

Source: http://www.messenger.com.ge/issues/1354_may_11_2007/n_1354_3.htm

[[Return to top](#)]

Food Sector

24. *May 12, Reuters* — **Pesticides next frontier in China food safety.** China's farmers overuse pesticides and have at their fingertips an array of banned and counterfeit products. Spraying chemicals on crops improperly or using products that may be fake or banned could lead to unsafe levels of residues in fruits and vegetables, experts say. China pledged last week to step up inspections in its food industry, saying checks on fertilizers and pesticides would be one of the priority areas. That comes after tainted animal feed exported from China led to the deaths of at least 16 cats and dogs in the U.S. and prompted a recall of more than 100 pet food brands, bringing the country's food safety standards under increased scrutiny. Part of the problem lies in the web of agencies who share responsibility for food safety. For pesticides, the Ministry of Agriculture monitors field use, the state planner and the Commerce Ministry grant production licenses, the Ministry of Health is responsible for setting maximum residue levels, and the State Environmental Protection Administration monitors environmental impacts. Producers are often small scale, and retailers are sometimes traveling salesmen, making monitoring nearly impossible.

Source: <http://www.reuters.com/article/newsOne/idUSPEK30160020070513>

25. *May 12, Agence France–Presse* — **Food safety an issue across Asia.** When Bangladeshi magistrate Rokon–ud–Dowla raided a local fish market to check on the quality of the food for sale, he was shocked by what he discovered. "We found all 176 tons of fish in the market containing harmful formaldehydes," he said. "We also sealed off dozens of bakeries and

confectionery shops for using textile and tannery dyes on sweets." Across Asia governments are struggling to control the use of toxic chemicals in manufactured and fresh food. Boric and benzoic acid, industrial dyes, fertilizers and pesticides, antibiotics, bad oil and sulphur dioxide are among the substances found in food throughout Asia. Experts across the region are beginning to blame a range of illnesses, including rising cancer rates, liver and kidney ailments, stunted mental and physical development in children — and, in extreme cases, death — on adulterated food. Among the most notorious violators of food safety standards is China, where two companies were found this month to have added a lethal chemical, melamine, to wheat gluten and rice protein which was later used in pet food believed to have killed dogs and cats in the U.S. Authorities in Shanghai have launched a mobile food testing van to tell whether food was safe to eat.

Source: http://news.yahoo.com/s/afp/20070513/lf_afp/asiahealthfoodda ngers_070513021759

26. *May 12, Food Consumer* — **Michigan firm recalls beef.** A Michigan firm is recalling about 129,000 pounds of beef products due to possible contamination with E coli. The beef products produced between March 1 and April 30 by Davis Creek Meats and Seafood, based out of Kalamazoo, MI, were shipped to foodservice distribution centers and Marketplace stores in Arkansas, Florida, Illinois, Indiana, Iowa, Kansas, Kentucky, Michigan, Missouri, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia and Wisconsin. The problem was discovered by Michigan Department of Community Health as part of an ongoing E coli illness investigation.

Source: http://foodconsumer.org/7777/8888/R ecalls_amp_A lerts_3/051207142007_Three_US_firms_recall_beef.shtml

27. *May 08, WCBD (SC)* — **Woman indicted for tampering with consumer products.** Karen Wyndham, of Cottageville, SC, was charged in a two count indictment with tampering with consumer products with reckless disregard for the risk and danger of bodily injury to others; and tampering with consumer products for the purpose of causing serious business injury. The Indictment alleges in Count 1 that on April 4, 2007, Wyndham recklessly and with disregard for the risk and danger of bodily injury to others, placed rodent poison into three previously sealed packages of ground beef, then placed the tainted meats in the meat display of a Super K-Mart store. Count 2 charges Wyndham with the tampering of consumer products with the intent to cause serious business injury.

Source: <http://origin.wcbd.com/midatlantic/cbd/news.apx.-content-articles-CBD-2007-05-09-0035.html>

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

Water Sector

28. *May 13, Israel21C* — **NATO funding Israeli system to safeguard world water supplies.**

Israel Schechter is a man with a dark secret. The Israeli scientist thinks he knows how a terrorist organization could conceivably contaminate a major American water supply. He's been working ever since the idea came to him, in an effort to develop a system that could prevent such an attack from succeeding. The researcher, from Israel's famed Technion Institute, is being backed by the North Atlantic Treaty Organization (NATO) and the Grand Water Research Institute (GWRI) which are financing the interdisciplinary research. According to Schechter,

the method he discovered emerged as a result of a role-playing exercise. The secret? Only a handful of a certain type of poison could be put into water sources and cause human fatalities despite the dilution factor. "Even if a terrorist used this idea, not that many people would actually die as a result — maybe 10 a day," said Schechter. "Even though the chances are low you would die, every time you would take a glass of water you'd worry." Schechter began to develop a device and monitoring facility that can not only detect chemical poisoning of water but neutralize it as well.

Source: <http://www.israel21c.org/bin/en.jsp?enDispWho=Articles%5E11649&enPage=BlankPage&enDisplay=view&enDispWhat=object&enVersion=0&enZone=Technology>

29. *May 12, Asia News* — **Drinking water shortage at Beijing Olympics.** Drinking water will not be available from taps for those residing outside the Olympic Village during next year's Olympics. It was the authorities that issued this warning, saying they wanted to guarantee safe water. The billions spent on cleaning and modernizing the Chinese capital have not been enough to make water potable. The vice-director general of the Beijing Water Management Bureau, Bi Xiaogang, said: "The quality of the water provided by the water plants is safe enough, but it is contaminated during the transfer process. We are still working on upgrading facilities. But in the Olympic Village we will provide safe drinking water from the tap." Xiaogang continued: "For the Olympics, Beijing will use reserves from the neighboring Hebei province, diverting up to 400 million cubic metres of water."

Source: <http://www.asianews.it/index.php?l=en&art=9231&size=A>

30. *May 09, Sandia National Laboratories* — **Unattended water sensor capable of 24/7 detection of toxins, bacteria in water supplies.** Sandia National Laboratories' unattended water sensor (UWS) has successfully undergone testing at a large California Bay Area water utility for more than a year and, just recently, has been deployed to a municipal water station in Arizona for additional observation and adjustments. Staff will perform periodic maintenance and troubleshooting on the system, which is expected to further demonstrate the viability of unattended water monitoring. Largely due to the automated sample preparation that is the hallmark of the device, the UWS is currently able to achieve sample analysis in just 12 minutes. According to Brent Haroldsen, who serves as Sandia's lead engineer on the project, the UWS is currently able to detect protein toxins such as SEB, botulinum, and ricin. Haroldsen said the next phase of the Sandia activities will be to expand the device's detection capability to include bacteria such as *E. coli* and protozoa such as *Cryptosporidium*. Sandia researchers, said Haroldsen, need to configure a working database of organism signatures to allow them to accurately distinguish the signatures from one another. He and his Sandia colleagues are looking at algorithm approaches that will help define the level of specificity the UWS will be able to achieve.

Source: http://www.sandia.gov/news/resources/releases/2007/watersens_or.html

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

Public Health Sector

31. *May 13, Jakarta Post (Indonesia)* — **Bird flu death reported in Indonesia.** A 26-year-old woman who tested positive for bird flu died at a hospital in Medan, North Sumatra, on

Saturday, May 12, pushing the Indonesia's human avian influenza death toll to 76. She died three days after being admitted to Adam Malik hospital. The resident of Deli Serdang regency was the second bird flu fatality at the hospital. Last week, a woman from Riau province who tested positive for the virus died at the hospital. Luhur Soeroso, the head of the hospital's bird flu management team, said both women tested positive for the H5N1 strain of the virus.
Source: http://www.thejakartapost.com/detailgeneral.asp?fileid=20070_513210725&irec=6

32. *May 13, Associated Press* — **United Nations' health chief faces test over bird flu cooperation.** Less than six months into her job as the United Nations' top health official, Margaret Chan faces a challenge. At issue are the sharing of samples of the H5N1 bird flu strain. The focus in recent months has been on negotiating a deal with Indonesia to resume sample sharing with the World Health Organization (WHO). Officials in the southeast Asian nation say the current system is unfair because the WHO passes virus samples on to drug companies for research purposes, but any vaccines developed from these specimens would likely be too expensive for many in poorer countries. The dispute has, for the time being, overshadowed concerns by health officials that China, whose large poultry stocks and vast territory make it an ideal breeding area for bird flu, is dragging its feet over the supply of virus samples to the WHO. Lack of cooperation, experts say, can slow efforts to track the disease and develop vaccines and other flu-fighting strategies.
Source: <http://www.ihf.com/articles/ap/2007/05/13/news/UN-GEN-UN-World-Health-Assembly.php>
33. *May 11, Agence France-Presse* — **Gabon takes measures in face of chikungunya virus.** Gabon's government said Friday, May 11, it had taken measures to protect against the chikungunya virus after initial tests indicated it had arrived in the western African nation for the first time. The government has mobilized teams of national experts and from the World Health Organization to develop strategies to combat the virus. A health ministry official told AFP that more than 5,500 cases have been counted over the last month in the province of Estuaire alone, which includes the capital Libreville.
Chikungunya information: <http://www.phac-aspc.gc.ca/msds-ftss/msds172e.html>
Source: http://news.yahoo.com/s/afp/20070511/hl_afp/gabonhealthepidemic_070511181933;_ylt=AjINkgIEN9G.wDZRvC5.m_qJOrgF
34. *May 08, U.S. Food and Drug Administration* — **FDA clears first respirators for use in public health emergencies.** The U.S. Food and Drug Administration (FDA) has cleared for marketing the first respirators that can help reduce the user's exposure to airborne germs during a public health medical emergency, such as an influenza pandemic. The two filtering facepiece respirators will be available to the general public without a prescription. The devices are also certified as N95 filtering facepiece respirators by the National Institute for Occupational Safety and Health (NIOSH). NIOSH certifies respirators for use in occupational settings in accordance with an appropriate respiratory protection program. An N95 filtering facepiece respirator is a type of face mask that fits tightly over the nose and mouth. It is made of fibrous material that is designed to filter out at least 95 percent of very small airborne particles. The filter and a proper fit determine the effectiveness of the product. Many companies make N95 respirators for workplaces, including health care settings. However, these respirators are the first devices to receive FDA clearance for use by the public during public health medical emergencies to reduce exposure to airborne germs.

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01630.html>

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

Government Sector

35. *May 14, Associated Press* — Elementary school horrifies students with fake gun attack.

Staff members of an elementary school in Murfreesboro, TN, staged a fictitious gun attack on students during a class trip, telling them it was not a drill as the children cried and hid under tables. The mock attack Thursday night, May 10, was intended as a learning experience and lasted five minutes during the weeklong trip to a state park, said Scales Elementary School Assistant Principal Don Bartch, who led the trip. "We got together and discussed what we would have done in a real situation," he said. But parents of the sixth-grade students were outraged. Some parents said they were upset by the staff's poor judgment in light of the April 16 shootings at Virginia Tech that left 33 students and professors dead, including the gunman. Principal Catherine Stephens declined to say whether the staff members involved would face disciplinary action, but said the situation "involved poor judgment."

Source: http://www.wusa9.com/news/news_article.aspx?storyid=58613

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

Emergency Services Sector

36. *May 14, Washington Post* — Many lessons in disaster drill. In the largest and most complex military and civilian training exercise of its kind, a 10-kiloton nuclear bomb detonated in greater Indianapolis, IN, killing 14,000 people, injuring 21,000, and overwhelming local responders. Thousands of local, state, and national forces -- including more than 2,000 National Guard members and 1,200 active-duty troops from U.S. Northern Command -- are taking part in the 11-day exercise this week. The preplanned scenario, designed to push the U.S. response system to the breaking point, has highlighted ongoing shortcomings in the government's ability to handle the aftermath of such a crisis. Nationwide, for example, the Army National Guard has only half the equipment it needs to respond to crises at home -- from terrorist attacks to natural disasters. The exercise showed new response capabilities, but it also revealed ongoing problems: radios and phones that malfunctioned, too few aircraft, and slow reaction times. Early decisions by the governor on whether to evacuate residents or shelter them in place had to be reversed hours later when expert advice became available, said Earl Morgan, director of public safety for Indianapolis. "That harms the public confidence."

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/13/AR2007051301134.html>

37. *May 11, Associated Press* — Mock nuclear disaster just the beginning for training site. The Muscatatuck Urban Training Center in Butlerville, IN, was the site of a simulated nuclear explosion this week -- a blast that in real life would have killed 6,000 instantly and severely injured thousands more. The mock disaster is just the beginning for Muscatatuck, a complex that includes 68 buildings, nearly 1,000 acres, and miles of roads and underground tunnels. The center could soon be home to up to 10 major training exercises each year -- some simulating

natural disasters or terrorist attacks on America and others portraying overseas urban warfare situations where soldiers face enemy combatants. The U.S. Army is investing \$97.3 million into the site, a former home for people with mental disabilities that closed in 2005 and was taken over by the Indiana National Guard. About 40,000 active and reserve soldiers could be trained at Muscatatuck every year by the time the site is fully operational in 2012.

Source: <http://www.jconline.com/apps/pbcs.dll/article?AID=/20070511/NEWS09/70511040>

[[Return to top](#)]

Information Technology and Telecommunications Sector

38. *May 14, IDG News Service* — **Verizon Business to acquire Cybertrust.** Verizon Communications' Business unit plans to acquire managed security vendor Cybertrust in an effort to pump up its cybersecurity offerings, Verizon announced Monday, May 14. The financial terms of the deal were not disclosed. The companies expect the transaction to close in 60 to 90 days. The goal of the acquisition is to make Verizon Business a leading provider of managed information security services to large business and government customers, Verizon said.
Source: http://www.infoworld.com/article/07/05/14/verizon-acquires-cybertrust_1.html
39. *May 14, Associated Press* — **DoD blocks some Websites.** Soldiers serving overseas will lose some of their online links to friends and loved ones back home under a Department of Defense (DoD) policy that a high-ranking Army official said would take effect Monday, May 14. DoD will begin blocking access "worldwide" to YouTube, MySpace and 11 other popular Websites on its computers and networks, according to a memo sent Friday by General B.B. Bell, the U.S. Forces Korea commander. The policy is being implemented to protect information and reduce drag on the department's networks, according to Bell.
Source: http://news.yahoo.com/s/ap/20070514/ap_on_hi_te/military_sites_blocked;_ylt=AgUInoY8fReoSkZDdOPh5.sjtBAF
40. *May 14, VNUNet* — **Google warns of Web malware epidemic.** A study released Monday, May 14, by Google has warned of "very high levels" of malware being hosted on Websites. In a year-long scan of over 4.5 million sites the Google team found code on 450,000 pages that could inject malware onto users' PCs via improperly patched browsers. A further 700,000 sites hosted similar code that, while not necessarily malicious, could harm the security of the PC viewing the page. "In most cases, a successful exploit results in the automatic installation of a malware binary, also called drive-by download," said the five-member team who wrote, "The Ghost in the Browser" paper. "The installed malware often enables an adversary to gain control over the compromised system and can be used to steal sensitive information such as banking passwords, to send out spam or to install more malicious executables over time." The research highlighted four main attack vectors: Web server security; user generated content; advertising; and third-party software.
Study: http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf
Source: <http://www.vnunet.com/vnunet/news/2189815/google-study-shows-scale-web>
41. *May 11, eWeek* — **Mother's Day brought unwanted spam.** Mother's Day brought unwanted

gift–spam. According to researchers at security vendor Sophos, spammers were trying to sell items like flowers, chocolates and baskets of fruit to consumers who may have not purchased presents for their mothers. Sophos experts said there are at least 23 different dates used in countries around the world to celebrate Mother's Day, but spammers focus on the North American celebration because it provides them with the largest possible audience. Meanwhile, security specialists at Panda Software's anti–malware laboratory, PandaLabs, on May 10 uncovered an application being used to control botnets in 54 countries. Ryan Sherstobitoff, product technology officer at Panda Software said the tool did not seem to be connected to the recent Mother's Day spam e–mails, but was a threat — particularly if it was used by cyber–criminals. "Everything has the end–all goal [of stealing] information," Sherstobitoff said. The application, called Zunker, contains a statistics section that includes graphs displaying the performance of each bot in the network, the number of available zombies and their monthly or daily activity.

Source: <http://www.eweek.com/article2/0,1895,2128934,00.asp>

- 42. *May 11, eWeek* — ANI Trojan lurks in popular hardware site.** More than a month after Microsoft patched the .ANI vulnerability, the popular Tom's Hardware has found the W32.ani Trojan lurking in one of its banner ads. ScanSafe, a managed Web security services company, on May 8 noticed a spike in traffic blocks that had a common theme. The company found that Tomshardware.com was unknowingly hosting the banner ad, which was redirecting users to a site where the driveby malware was automatically downloaded. The banner ad was up, infecting victims with unpatched systems, for 24 hours.

Source: <http://www.eweek.com/article2/0,1895,2128813,00.asp>

Internet Alert Dashboard

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

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

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[[Return to top](#)]

General Sector

Nothing to report.

[[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.