



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 08 March 2005

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

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

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

Daily Highlights

- The Salt Lake Tribune reports a railroad tanker car leaking a mixture of chemicals sent a plume of orange fumes above South Salt Lake City on Sunday, causing the evacuation of as many as 6,000 residents and the closing of Interstate 15. (See item [2](#))
- The Nebraska State Government reports Governor Dave Heineman unveiled Nebraska's new Biocontainment Unit at the University of Nebraska Medical Center in Omaha; there are only two other biocontainment patient care units in the country. (See item [23](#))
- The Business Journal of Portland reports the Department of Homeland Security has chosen Portland, OR, and Phoenix, AZ, as the two sites for TopOff 4, the tests that ascertain ways that top federal, state and local officials handle major security-breaching events. (See item [26](#))

DHS/IAIP Update *Fast Jump*

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

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

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

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

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

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

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *March 04, SecurityFocus* — **Companies resist nuclear cyber security rule.** Companies that make digital systems for nuclear power plants have come out against a government proposal that would attach cyber security standards to plant safety systems. The 15-page proposal, introduced by the Nuclear Regulatory Commission (NRC), would rewrite the commission's "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." The current

version, written in 1996, is three pages long and makes no mention of security. The plan expands existing reliability requirements for digital safety systems, and infuses security standards into every stage of a system's lifecycle, from drawing board to retirement. Last month the NRC extended a public comment period on the proposal until March 14th to give plant operators and vendors more time to respond. So far, industry reaction has been less than glowing. Capri Technology, a small California firm that builds specialized systems and software for nuclear plants, calls the regulations "premature," and says the proposal could deter plant operators from installing new digital safety systems entirely. Last year the United Nations' International Atomic Energy Agency (IAEA) warned of growing international concern about the potential for cyber attacks against nuclear facilities, and said it was finalizing new security guidelines of its own.

Source: <http://www.securityfocus.com/news/10618>

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

Chemical Industry and Hazardous Materials Sector

- 2. *March 07, Salt Lake Tribune (UT)* — Toxic chemical spill forces thousands to evacuate in Utah.** A railroad tanker car leaking a mixture of chemicals sent a plume of orange fumes above South Salt Lake City, UT, the morning of Sunday, March 6, causing the evacuation of as many as 6,000 residents and the closing of Interstate 15. Workers found acid bubbling from three holes in the tanker Sunday morning in the Roper Train Yard. Special equipment was brought in from Las Vegas, NV, around 10:00 p.m. to pierce the tanker and drain the liquid into other containers. More than 100 emergency crews from as far away as Tooele, UT, responded to the chemical spill, which they were initially told was composed of sulfuric, nitric, hydrofluoric and hydrochloric acids. The chemicals are dangerous on a number of levels — any one of them could burn the skin on contact, and if inhaled could damage the lungs, esophagus, cause difficulty breathing, nausea and vomiting. By 10:00 p.m. Sunday night, after hours of confusion, miscommunication and finger pointing, residents were allowed to return home. The Federal Bureau of Investigation was at the scene and determined the leak wasn't linked to any type of terrorist or criminal activity.

Source: http://www.sltrib.com/ci_2598382

- 3. *March 07, WBEX (OH)* — Chemical spill prompts road closure in Ohio.** A tanker truck crashed Monday morning around 4:30 a.m., March 7, spilling a liquid plastic additive considered a fire hazard and snarling commuter traffic on U.S. 23 near Kingston and Chillicothe, OH. U.S. 23 just north of Chillicothe reopened around 11:00 a.m., but northbound remained closed at the time.

Source: http://www.wbex.com/cc-common/feeds/view.php?feed_id=188&feed=/localnews.html&instance=1&article_id=16616

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

Defense Industrial Base Sector

- 4.**

March 07, Bloomberg — **British contractor acquires U.S. asset.** BAE Systems Plc, Europe's largest defense contractor, agreed to buy United Defense Industries Inc. for \$3.97 billion to tap growing demand for artillery and armor, including the Bradley Fighting Vehicle used by the U.S. in Iraq. BAE will pay \$75 a share in cash for Arlington, VA– based United Defense, Chief Financial Officer George Rose said on Monday, March 7. London–based BAE will become the Pentagon's sixth–largest contractor with the purchase, which will be the biggest defense–industry acquisition in more than four years and the biggest ever by a foreign company in the U.S. BAE bought five U.S. defense companies last year. Spending on tanks and armored vehicles is growing in the U.S. and Europe because of conflicts such as those in Iraq and Afghanistan. The defense budget last year in the U.S., the world's largest weapons market, was \$375 billion, about three times that of the U.K., France, Germany and Italy combined. “The acquisition fits the strategy BAE laid out to develop in the U.S. with the Department of Defense,” said Zafar Khan, an analyst at Societe Generale.

Source: http://www.bloomberg.com/apps/news?pid=10000087&sid=a0m1de6tDxEc&refer=top_world_news

[[Return to top](#)]

Banking and Finance Sector

- March 07, New Zealand Press Association* — **Internet banking in New Zealand under scrutiny after hacker accesses accounts.** In New Zealand, police, a consumer–watchdog and two major banks are warning people to be extra cautious in using the Internet for banking. Police e–crime national manager Marten Kleintjes said on Sunday, March 6, Internet banking was becoming increasingly risky and many banks needed to tighten security for such services. The warning follows the discovery a hacker had installed software at a Wellington Internet cafe, and thus gathered the usernames and passwords of people banking online at the premises. It took the hacker three minutes to install the hidden software last month, and in the following weeks he gained access to accounts with balances totaling more than US\$367,000. By using a widely available key–logging program that recorded every key typed on a computer when a bank's Web address, customer ID and password were entered, they were automatically saved and e–mailed to the hacker. Consumers' Institute director David Russell said people needed to be vigilant at tracking Internet banking transactions, and while some banks had improved security, others needed to do something fast.

Source: http://www.nzherald.co.nz/index.cfm?c_id=5&ObjectID=10113938

- March 07, eWeek* — **Private sector, government team up against phishing.** When phishing emerged as a serious problem in 2003, many law enforcement agencies were caught off guard. The Internet boom had spawned special task forces staffed with investigators trained in electronic crimes, but these teams were uniformly understaffed and overburdened. As a result, the FBI and the Secret Service have relied on the private sector for a great deal of help in tracking down phishing sites and taking them offline. The Internet Crime Prevention & Control Institute (ICPCI), a joint project of the University of Miami and Zero Spam Network Corp., has been working with federal authorities for nearly a year on this task. “The feds have a prosecution–driven culture, so a crime has to be committed for them to get involved. And there are more economic crimes of a sizable nature than there are resources,” said Bill Franklin, president of Zero Spam, of Coral Gables, FL. “We're usually trying to stop it before there's a

loss, and that's hard for them to justify devoting resources," said Franklin.

Source: <http://www.eweek.com/article2/0.1759.1772524.00.asp>

- 7. *March 04, eSecurity Planet.com* — U.S. government reaching out to other countries to combat cyber crimes.** The U.S. government is teaming up with security industry leaders to reach out to foreign countries and help them tackle the growing global problem of cyber crime. U.S. law enforcement agents and prosecutors have been working hard to capture and prosecute virus authors, spammers and the people behind online identity theft schemes in the U.S., however, that's just taking a bite out of a larger worldwide problem. Countless other cyber criminals who live outside the country are beyond the reach of U.S. agents, who may only aid foreign investigations — when the assistance is welcome. That, some security experts say, is leaving U.S. corporations and users more open to attack. Chris Painter, deputy chief of the Computer Crime and Intellectual Property Section at the Department of Justice, who also chairs the G8 High-Tech Crime SubGroup, says he has been working with others in the U.S. government to reach out to foreign governments and develop needed relationships. Painter says getting various countries to work together to define the problem and discuss courses to take is a key first step in ultimately sharing information and mutually aiding investigations and prosecutions.

Source: <http://www.esecurityplanet.com/trends/article.php/3487751>

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

Transportation Sector

- 8. *March 07, USA TODAY* — Uneasy airline executives anticipate \$60-a-barrel oil.** Jittery airline executives, having already raised fares and cut flights, are now looking ahead to the possibility of \$60-a-barrel oil. Last week, crude oil prices increased to within 50 cents of October's \$55.67-a-barrel record. Recent decisions by large airlines to raise fares by up to \$20 round trip won't cover the added costs in fuel prices, says consultant David Swierenga of Vienna, VA. Despite an expected increase in passengers, Swierenga now looks for the industry to lose as much as \$2.5 billion this year, driving cumulative losses since 2000 to \$33 billion. The surge in oil prices is already having an impact. A week ago, US Airways, which is operating in bankruptcy protection, quit flying routes it had just launched from Fort Lauderdale — to San Juan, Puerto Rico, Panama City, and San Salvador. US Airways cited fuel costs and weak bookings. Most big airlines are defenseless against increases in fuel prices because they lack the cash or financial credibility to hedge prices, or to lock in a future price by contract. Neither US Airways nor Delta Air Lines has fuel hedges this year. Among major airlines, only discount leader Southwest is well protected, with 85% of its fuel this year hedged at \$26 a barrel.

Source: <http://www.usatoday.com/travel/flights/2005-03-06-jetfuel-us at x.htm>

- 9. *March 07, Los Angeles Daily News* — Train tables are a safety issue on California's Metrolink trains.** Stationary tables on California's Metrolink trains pose the risk of severe injury to passengers in a crash, federal rail officials say, and they are working to design work surfaces that would "give" on impact. Federal investigators say two passengers died of traumatic injuries likely suffered when they hit the tables during a 2002 Metrolink crash in Placentia, CA. And the lawyer for a former Santa Clarita woman left paralyzed during a 2003

wreck in Burbank blames the workstation for her injuries. The safety issue came into the spotlight again this past January, when 11 passengers were killed and nearly 200 injured in a freak crash involving two Metrolink trains in Glendale. Realizing the risk to passengers, federal authorities are working to design a table with edges that would crush on impact, but say it could take years to get the necessary approvals. Metrolink is working separately on a design with a more flexible wall attachment and hopes to have a model that could be installed on its trains within six months — if the money can be found. Some officials say the issue could be addressed simply by installing seat belts on the trains.

Source: <http://www.dailynews.com/Stories/0.1413,200~20954~2748455.00.html>

10. *March 07, Washington Post* — Border still easily crossed. The U.S. Border Patrol in New Mexico has motion sensors buried in the ground and high-resolution infrared cameras mounted on poles. On the ground, agents in big sport-utility vehicles are armed with night-vision goggles and satellite global positioning devices. Helicopters fly up and down the border, shining powerful spotlights. Every day of the year, such high-tech barricades help U.S. authorities catch more than 3,000 people along the 2,000-mile U.S.-Mexico border. Yet despite the unprecedented investment in technology and manpower, illegal immigrants are still coming in waves — and their numbers are increasing. U.S. officials made over one million apprehensions along the border last year, a 24 percent increase over the year before. The officials said they have caught more than 53,000 people with criminal records — including about 9,000 felony offenders — since September, when a new computerized system was started to allow agents to quickly check a migrant's background against the FBI's database. But experts in both countries estimate that perhaps 500,000 or more still make it through each year. How to better manage the contentious issue of immigration will top the agenda when President Bush meets with Mexican President Vicente Fox later this month in Texas.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A12368-2005Mar 6.html>

11. *March 07, Department of Transportation* — Grants to fund safety and improvements at North Carolina airports. Federal grants totaling approximately \$62.9 million will help to enhance safety, upgrade terminal buildings and expand capacity at airports throughout North Carolina, U.S. Transportation Secretary Norman Y. Mineta announced on Monday, March 7. Ten airports and the state will receive money for projects that include building and rehabilitating runways, building new terminals and adding fire and rescue equipment, among other projects. The funds come from the Airport Improvement Program of the U.S. Department of Transportation's Federal Aviation Administration.

Source: <http://www.dot.gov/affairs/dot4005.htm>

12. *March 07, New York Times* — Radio tags useful for finding stray bags. For the last several years, the airlines have envisioned using new radio frequency identification, or RFID, tags that identify and track items with a precision unmatched by today's bar code scanning systems. Advocates of the new technology say that it is ready for use but very expensive. Yet by some estimates, the investment needed to move to radio tag technology could be recouped remarkably quickly. Today's bar code scanning systems fail to identify as many as 15 percent to 20 percent of the bags moving past automated checkpoints, leaving increasingly understaffed baggage handling crews to identify visually bags by their tags and to redirect them to the proper flights. The industry tracks its bag-handling performance by measuring bags lost per 1,000 customers. While that number was below five in 2004, that still adds up to millions of bags

going astray annually. Chasing down misdirected luggage and paying claims on lost bags can cost \$100 to \$200 a bag, according to industry estimates. In test projects at airports, RFID systems, which use scanners to read codes embedded in microchips sealed inside plastic tags, have accurately identified bags 95 percent of the time they passed a scanner.

Source: <http://www.nytimes.com/2005/03/07/technology/07baggage.html>

13. *March 07, Reuters* — **International Air Transport Association says 2004 safest year for air transport.** Last year was the safest since 1945, the start of large-scale commercial air traffic, for commercial air transport, both in terms of passengers killed and aircraft destroyed or irreparably damaged, the industry's global body International Air Transport Association (IATA) said on Monday, March 7. IATA data showed the chances of dying in an airline accident in 2004 were one in every 10 million people flying against nearly three in 2002 and more than seven in 1996. The figures took account of varying passenger numbers over the years. Just under eight airliners were destroyed or irreparably damaged for every 10 million sectors flown — industry jargon for the distance covered between a take-off and a landing — compared to more than nine in 2002 and 13 in 1996. "2004 was the safest year ever for air transport," said IATA director general Giovanni Bisignani, hailing the figures as a victory for the body in a campaign to increase air safety. "The industry continues to invest in our top priority with fantastic results," Bisignani said in a statement, adding this had been achieved despite accumulated losses by airlines of \$35 billion since 2001.

Source: <http://www.alertnet.org/thenews/newsdesk/L07707544.htm>

14. *March 06, GovExec* — **September 11 commissioners seek revised aviation security report.** A former member of the 9/11 commission this week called on the administration to revise a report on aviation security before the September 11, 2001, attacks so it does not contain redacted sections. The third staff report from the 9/11 commission was released by the administration last month, even though it was completed in August. Parts of the report, however, were redacted, making it the only part of the commission's work that was not released in its entirety. The report, called "The Four Flights and Civil Aviation Security," examines aviation warnings prior to the 9/11 attacks and failures within the aviation security system that contributed to the attacks. Report:

http://www.archives.gov/research_room/research_topics/staff_report_3.pdf

Source: <http://www.govexec.com/dailyfed/0305/030405c1.htm>

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

Postal and Shipping Sector

15. *March 07, WEEK-TV (IL)* — **Suspicious package found at Illinois post office.** A hazardous materials team was called to Peoria, IL, main post office Monday, March 7, to investigate a suspicious package. Peoria Fire Department Battalion Chief Doug Brignall says their field tests have come back negative so far. Brignall says a postal worker noticed a white powder in a regular business envelope. The envelope was immediately isolated in a bulk mail room and the authorities were notified. Brignall says they're taking every precaution, but all signs are pointing to it being a hoax. Another sample will be sent to a lab for testing.

Source: <http://week.com/morenews/morenews-read.asp?n=7379>

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

Agriculture Sector

16. *March 06, Associated Press* — Fungus poses threat to Oregon's hazelnut crop. Authorities have discovered a deadly fungus on the branches of the United States' oldest commercial hazelnut orchard. The Eastern filbert blight has in the past decimated Oregon's hazelnut industry and as recently as last year led to a quarantine of affected orchards. The trees at the Dorris Ranch orchard date to 1903, and more than half of all commercial filbert trees in the U.S. originate from the ranch's nursery stock. Agriculture officials have urged property owners to cut and burn diseased trees, and some have complied. Others have ignored the warnings, allowing the disease to fester and spread to commercial orchards. At Dorris Ranch, officials say the regimen of scouting for pustules, pruning infected wood and spraying will now be a permanent chore. "It's here and it's never going to be eradicated," Dorris Ranch orchard manager Garry Rodakowski said. The fungus emerges as rows of small, black cankers on limbs, eventually girdling infected branches and killing the leaves. It can result in an unproductive orchard in three to seven years and kill the trees in five to 12 years.

Source: http://159.54.226.83/apps/pbcs.dll/article?AID=/20050306/STA_TE/50306002/1042

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

Food Sector

17. *March 04, Reuters* — WHO says acrylamide levels in foods should be cut. The World Health Organization (WHO) said on Friday, March 4, people should eat less acrylamide, a chemical associated with fried foods that has caused cancer in rats, because of a potential threat to health. It called on national governments to urge their food industries to "lower significantly" the acrylamide content in foods such as French fries, potato chips, coffee, and cereals-based products including bread. Acrylamide is formed when certain foods, particularly plant-based foods that are rich in carbohydrates and low in protein, are cooked at high temperatures. But because amounts can vary dramatically in the same foods, depending on factors such as cooking temperature and time, it was impossible to issue recommendations about how much of a specific food it was safe to eat, the WHO said.

Source: <http://www.alertnet.org/thenews/newsdesk/L04365439.htm>

18. *March 04, USAgNet* — Vietnam reopens markets to U.S. beef. The government of Vietnam has reopened its markets to U.S. beef. Vietnam closed its markets in 2003, following the confirmation of the first and only case of bovine spongiform encephalopathy in a Washington state dairy cow. The U.S. Meat Export Federation said that although Vietnam is a small market for U.S. beef it is one of the first Asian countries to reopen its markets to U.S. beef.

Source: <http://www.usagnet.com/story-national.cfm?Id=242&yr=2005>

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

Water Sector

19. *March 07, Environmental Protection Agency* — **Agency officials to increase monitoring requirements for lead in drinking water.** The Environmental Protection Agency announced Monday, March 7, that it is initiating the Drinking Water Lead Reduction Plan to strengthen, update and clarify existing requirements for water utilities and states to test for and reduce lead in drinking water. This action, which follows extensive analysis and assessment of current implementation of regulations, will tighten monitoring, treatment, lead service line management and customer awareness. The plan also addresses lead in tap water in schools and childcare facilities to further protect vulnerable populations. Lead is a highly toxic metal that was used for many years in products found in and around homes. Even at low levels, lead may cause a range of health effects including behavioral problems and learning disabilities. Children six years old and under are most at risk because this is when the brain is developing. The primary source of lead exposure for most children is lead-based paint in older homes. Lead in drinking water adds to that exposure.

Source: <http://yosemite.epa.gov/opa/admpress.nsf/b1ab9f485b098972852562e7004dc686/e8e0702362bb3df685256fbd005aaf0b!OpenDocument>

[[Return to top](#)]

Public Health Sector

20. *March 07, Washington Post* — **Global Secure buys California software firm.** Global Secure, a Washington, DC, homeland security company, paid \$20 million in cash and stock last week for a California maker of software that alerts state and municipal health officials and hospitals to bioterrorism and other urgent threats. Craig Bandes, chief executive of Global Secure, said Virtual contributes to a suite of products offered to state and local governments to use in an emergency such as a terrorist attack. Virtual, founded in 2001, has 45 employees and contracts with public health agencies in 16 states and the District of Columbia.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A12668-2005Mar 6.html>

21. *March 07, New York Times* — **Analyzing New York City's air.** Dr. J. Craig Venter has embarked on an exploration of New York City air. In a pilot project scheduled to be officially announced Monday, March 7, a team from Venter's nonprofit organization, the J. Craig Venter Institute, is using a filtering device to take air samples from atop the roof of a 40-story office building in the most congested part of Midtown. The filters are then sent to the institute's Joint Technology Center in Rockville, MD, where city air is broken down to its most minute particles, revealing for the first time the genetic material of the microbes and other organisms that New Yorkers normally breathe. While much is known about various pollutants, only a tiny percentage — about one percent — of the micro-organisms in the air can be identified by traditional methods involving growing cultures. The new process is intended to provide as intimate a picture of the air as the genome mapping provided of the human body. The genetic information could then be used to create a comprehensive background image of New York's air. In turn, that would make it easier to identify any dangerous new organisms that come from an act of bioterrorism.

Source: <http://www.nytimes.com/2005/03/07/nyregion/07air.html>

22.

March 07, Associated Press — **Nurse contracts bird flu in Vietnam.** A 26-year-old nurse who cared for a bird flu patient has contracted the virus, but it's unclear whether he caught the disease from his patient, a Vietnamese health official said Monday, March 7. The nurse — Vietnam's fifth case in the past two weeks — is more likely to have caught the disease outside the hospital, the health official said. The man was from northern Thai Binh province, the site of four of the five recent cases. He is the first medical worker known to have been infected by the disease. "We are investigating this case," said Pham Van Dui, director of the provincial Preventive Medicine Center. "But it's more likely that he contracted the disease while visiting his girlfriend in the district during Tet where poultry were served and bird flu outbreaks were reported," he said. Fourteen people have died in Vietnam since the bird flu reemerged in the country at the end of last year. Vietnam has had the highest total number of deaths from the disease — 33 so far.

Source: <http://sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/03/07/international/i003042S98.DTL>

23. *March 07, Nebraska State Government* — **Nebraska Governor unveils biocontainment unit.** Governor Dave Heineman unveiled Nebraska's new Biocontainment Unit at the University of Nebraska's Medical Center (UNMC) Monday, March 7, in Omaha. There are only two other biocontainment patient care units in the country. The U.S. Army Medical Research Institute of Infectious Diseases houses a two-bed special Bio-safety patient care suite at Fort Detrick, MD, for military members and investigators who may be exposed to infectious agents, and the U.S. Centers for Disease Control and Prevention has a two-bed unit at Emory University Hospital in Atlanta, GA. Glenn Fosdick, president of UNMC, said, "This unit allows us the opportunity to help hospitals across the country care for patients who come into contact with deadly, highly contagious diseases. If an outbreak occurs in another state, we will be here ready and able to take patients who need this specialized care." The new unit is on the same campus as the state's Bio-safety Level-3 laboratory. The collocation will allow timely diagnosis and treatment of patients who come into contact with diseases like smallpox, avian flu, or botulism.

Source: http://gov.nol.org/news/2005_03/07_cdc.html

24. *March 05, New York Times* — **FDA seizes millions of pills from pharmaceutical plants.** Concerned about quality-control problems, the Food and Drug Administration (FDA) used armed federal marshals to seize millions of tablets of two medicines from facilities in Tennessee and Puerto Rico operated by GlaxoSmithKline, the agency said Friday, March 4. The drugs are the antidepressant Paxil CR, which had \$725 million in sales last year and is used by some 450,000 patients in the U.S. each month; and Avandamet, a diabetes medicine, whose sales are undisclosed but are far smaller. The FDA said that neither pill was medically necessary and that many alternatives existed for both. It added that it knew of no patients harmed by the poorly made pills and said patients could safely take any pills they had left. Officials at both the agency and GlaxoSmithKline said they could not predict when or how the manufacturing problems would be resolved, though the company said it satisfied the agency's concerns about Paxil CR last November. Despite the absence of evidence that the pills had harmed anyone, the agency said, a drug maker must be able to assure the public that its products are properly made.

Source: <http://www.nytimes.com/2005/03/05/politics/05drug.html?oref=login>

25. *March 01, University of Florida* — **New approach could bolster antibiotic arsenal.**

University of Florida researchers have devised a method that combines testing of various drug

concentrations at the site of infection with a series of laboratory analyses and mathematical models designed to streamline drug development. The method helps better determine which drugs are worth studying in people and at which dose, avoiding the typically lengthy and expensive trial-and-error approach that can take years. In recent years, scientists worldwide have sounded the alarm: There simply aren't enough drugs to combat bacteria. Yet designing and testing new antibiotics can be a slow and costly process, said Hartmut Derendorf, chairman of the department of pharmaceuticals at the University of Florida College of Pharmacy. "About one new antibiotic a year is approved," said Derendorf. "That's certainly not enough. Even more worrisome, there are very few in the pipeline right now." About 70 percent of bacteria found in hospitals resist at least one of the drugs commonly used to treat the infections they cause, according to the Food and Drug Administration. The agency warns that unless problems are detected early and swift action taken to find substitute drugs, previously treatable diseases could again emerge in more virulent forms.

Source: http://news.health.ufl.edu/stories/2005/Mar/Bug%20Drugs.shtm_l

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

Government Sector

Nothing to report.

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

Emergency Services Sector

26. *March 06, The Business Journal of Portland (OR)* — Portland picked as site for terror exercise. The Department of Homeland Security (DHS) has chosen Portland, OR, and Phoenix, AZ, as the two sites for "TopOff 4," a shorthand term for tests that ascertain ways that top federal, state and local officials handle major security-breaching events. TopOff 4 is scheduled for May 2007. The designation means that several drills — testing preparedness for attacks involving biological, radiological and various explosives—could occur in and around Portland, said Miguel Ascarrunz, the city's Office of Emergency Management director. DHS has yet to determine exactly which tests will occur in Portland. Ascarrunz said the TopOff 2 exercise held in King County, WA, in 2003 cost around \$1.5 million. Oregon hopes to fund the drills with various Homeland Security grants targeted for local exercises, as well as corporate donors. Ascarrunz wants Oregon's business community to provide key input as the region develops its plans. Ascarrunz said his department will devote four full-time officers to work on the 2007 program. He also wants to enlist law enforcement agencies from throughout the state, as well as Clark County, WA, to help prepare for the Homeland Security tests.

Source: http://www.bizjournals.com/portland/stories/2005/03/07/story_1.html?GP=OTC-MJ1752087487

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

Information Technology and Telecommunications Sector

27.

March 07, IDG News Service — **Terrorists target India's outsourcing industry.** India's software and services outsourcing industry is a likely target for a terrorist group operating in the country, local police warned on Sunday, March 6. But Indian outsourcing and software companies said they are prepared to cope with the threat. Documents seized from three members of the Lashkar-e-Toiba (LeT) terrorist group killed in an encounter with the police on Saturday, March 5, revealed that they planned to carry out suicide attacks on software companies in Bangalore, Karnal Singh, joint commissioner of police in Delhi, told reporters. LeT is demanding independence for the Indian state of Jammu and Kashmir. "The terrorists planned to hit these companies in an effort to hinder the economic development of the country," Singh said. IBM, Intel, Texas Instruments, Accenture, Wipro, and Infosys Technologies are among those with operations in Bangalore. Most of the technology companies in the city have already set up disaster recovery plans and special disaster recovery sites that could be used in the event of a terrorist attack, according to Kiran Karnik, president of the National Association of Software and Service Companies in Delhi.

Source: http://www.infoworld.com/article/05/03/07/HNterroristsindia_1.html

28. *March 06, CNET News* — **Telephone numbers assigned to unlicensed Internet phone company.** The caretaker for North America's 10-digit telephone numbers recently assigned a few thousand numbers to an unlicensed Internet phone company, a sign the agency is willing to deal directly with a new generation of communication providers. Until being approached by Net phone operator LibreTel, the North American Numbering Plan Administration distributed numbers only to entities with government telephone operator licenses. However, LibreTel is unlicensed, like most other providers of voice over Internet Protocol (VoIP). Typically, VoIP providers must get phone numbers from intermediaries like local phone companies.

Source: http://news.com.com/Dialing+without+a+license/2100-1037_3-5601592.html?tag=nefd.top

29. *March 05, SecurityFocus* — **Windows Server 2003 and XP SP2 LAND attack vulnerability.** Windows Server 2003 and XP SP2 (with Windows Firewall turned off) are vulnerable to a Denial of Service through a LAND attack. A LAND attack occurs when a user sends a TCP packet with SYN flag set and source and destination IPs are the same and source and destination ports are the same, using the target system IP address. Enable Windows Firewall as a workaround.

Source: <http://www.securityfocus.com/archive/1/392354/2005-03-03/2005-03-09/0>

30. *March 04, InformationWeek* — **White House report shows improvement in IT security.** Government auditors certified and accredited 77% of the federal government's 8,623 IT systems after undergoing risk assessments and security-control testing last fiscal year, up from 62% in fiscal year 2003, according to a White House report to Congress made public Friday, March 4. Several agencies, notably the departments of Labor and Transportation, showed remarkable improvements, with Transportation certifications rocketing to 98% from 33% and Labor accreditations leaping to 96% from 58%. Karen Evans, administrator for E-government and IT in the White House Office of Management and Budget, said at a press briefing that she was pleased with the progress, but the government must be diligent even when all systems are eventually certified. "You can't be 100% secure," she said. Report:

http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf

Source: <http://www.informationweek.com/story/showArticle.jhtml?articleID=60405791>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: Multiple variants of the Beagle worm have emerged over the past few days and are becoming a rather sizeable threat in terms of infection rate. Many of these variants are being reported as a mass-mailing worms that uses its own SMTP engine to send out copies of the tooso trojan. The US-CERT suggests ensuring that updated anti-virus signatures have been deployed to machines on your network. For more information on the Beagle worm and the tooso trojan, please see the following link:

<http://securityresponse.symantec.com>

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 139 (netbios-ssn), 1025 (----), 1026 (----), 1027 (icq), 80 (www), 53 (domain), 137 (netbios-ns), 25 (smtp) 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/IAIP Products & Contact Information

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

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source

published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

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

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

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

Contact DHS/IAIP

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

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

DHS/IAIP Disclaimer

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