



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 30 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 Associated Press reports a University of California, Berkeley, computer laptop containing personal information on at least 98,000 alumni, graduate students and past applicants has been stolen. (See item [10](#))
- The Journal News reports a man was arrested at New York's Westchester County Airport on Monday, when he tried to board a plane with a piece of explosive detonating cord in his carry-on luggage. (See item [12](#))

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 29, Associated Press* — **Worker with false documents hired by nuclear plant in Iowa.** The U.S. Attorney's office says a 31-year-old Mexican national with false documents was hired to perform pipe insulation work at Duane Arnold nuclear plant in Palo, IA. Gerardo Estrada-Gallegos was arraigned Monday, March 28, on four counts of possessing false documents, two counts of using false documents to gain employment and one count of making false statements to a federal agency. According to a statement, Estrada-Gallegos was hired by the nuclear plant to perform work, however, discrepancies in the documents turned up during a security check. Renee Nelson, a plant spokeswoman, told The Associated Press that the worker was hired by a subcontractor.

Source: <http://www.whotv.com/Global/story.asp?S=3135189>

2. *March 29, San Diego Union-Tribune* — **Southern Californians need to conserve to get through summer.** Electricity supplies in California should be adequate but tight for typical summer conditions, according to a report by the California Independent System Operator (ISO), which oversees grid reliability for much of state. The report found that supplies would fall short by about 1,700 megawatts during an extraordinarily hot season. The ISO projects considerably larger reserve margins of electricity supply in Northern California than in the southern part of the state. Even for its projections of the hottest likely summers, margins in Northern California are expected to stay well above the seven percent reserves considered prudent by power officials, according to the ISO. Despite improvements in transmission lines linking north and south, there are still relatively tight constraints on moving power between the two regions. For that reason, the more-than-adequate reserve margins projected for Northern California still can't be fully tapped to meet the demands of Southern California, where projections are that margins would fall to zero or below during a so-called one-in-10 summer heat wave. At those times, reducing demand would be key. "We don't anticipate having a need for blackouts or rolling outages, but the reserve margins are not as great we like," said Gregg Fishman, a spokesperson for the ISO. Summer Operations Assessment: <http://www.aiso.com/docs/09003a6080/35/46/09003a60803546fd.pdf>
Source: http://www.signonsandiego.com/news/business/20050329-9999-1b_29power.html
3. *March 29, Indianapolis Star (IN)* — **Midwest Independent Transmission System Operator to begin operations soon.** The Midwest Independent Transmission System Operator, or MISO, in less than four days will begin full operations to direct the complex movement of power and manage the price of electricity in 15 states and a Canadian province. At a cost of \$400 million to build, MISO is intended to improve the reliability of the grid and potentially save consumers hundreds of millions of dollars a year. MISO will settle an estimated \$1.5 billion a month in wholesale power sales among power generators, banks, power traders and others in the industry. MISO executives said everything is ready for 24-hour monitoring and pricing operations to begin April 1. However, just in case, they are running last-minute tests for the 600 employees and the state-of-the-art Carmel, IN, headquarters. Power experts hope the MISO system of sending pricing signals through the market will help to reduce congestion and inefficient transmission. But they also hope MISO will create a financial incentive to build new long-distance power transmission lines to carry more power for the growing Midwest. MISO will be huge, with 1,400 generating stations and 80,000 megawatts of typical load.
Source: <http://www.indystar.com/articles/4/232800-1994-223.html>
4. *March 28, Associated Press* — **Nuclear plants using dry casks for spent fuel.** About 40 percent of the nation's nuclear power plants have begun moving spent fuel out of cooling pools and into massive dry casks, embracing a storage approach that a National Academy of Sciences panel said offers safety advantages. The nation's 64 active nuclear power plants, which together house 103 reactors, all now store nuclear waste in pools of water after it is removed from reactors. Eventually, the spent fuel is supposed to be shipped to a national nuclear waste repository planned for Yucca Mountain in Nevada. As Yucca Mountain has been delayed, utilities are increasingly moving some of the waste from pools to huge metal or metal-and-concrete casks. That method is now employed at about 25 active U.S. nuclear power plants, according to the Nuclear Energy Institute, the industry trade group. Watchdog

groups contend the casks are safer than the pools, especially when the pools reach capacity. However, the dry casks are more expensive — a cost that would be born by the power plant owners and the government.

Source: http://news.yahoo.com/news?tmpl=story&u=/ap/20050328/ap_on_re_us/nuclear_waste_1

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

Chemical Industry and Hazardous Materials Sector

5. *March 29, Channel Cincinnati.com (OH)* — **Propane leak in Kentucky prompts evacuations.** Hazmat crews responded to the scene of a propane leak in Crestview Hills, KY, Tuesday, March 29. Investigators said a construction worker was using a crane to move a tank of propane outside the Crestview Hills Mall. The crane malfunctioned and the tank fell, causing the leak. Dixie Highway was closed between Dudley and Interstate 275 for about five hours. The road reopened shortly before 5 p.m. Several restaurants in the area were closed, but the Dillard's remained open for business. Neighborhoods were not evacuated because officials said residents were not in danger. Investigators said about 400 gallons of propane leaked from the 1,000-gallon tank, but it was only half full. They were able to close off the leak and keep about 100 gallons still inside. No injuries were reported and no one got sick from the gas, Longnecker reported.

Source: <http://www.channelcincinnati.com/news/4327023/detail.html>

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

Defense Industrial Base Sector

6. *March 28, Reuters* — **Pentagon takes over responsibility for Air Force acquisitions.** The Department of Defense said Monday, March 28, it has taken over temporary responsibility for running the top 21 weapons-buying programs of an Air Force that has lost its top three civilian officials since January amid a procurement scandal. The projects, totaling about \$180 billion, involve such leading U.S. defense contractors as Lockheed Martin Corp., Boeing Co., Northrop Grumman and Raytheon Co. In assuming personal authority over the programs, at least several of which are over budget and vulnerable to cuts or stretch-out, Michael Wynne, the Pentagon's chief weapons buyer, said "this action is not a punitive one. Rather it is meant to assist the Air Force by overseeing and providing advice on important Air Force programs during a time of transition," he said in a statement. Wynne said he had no date in mind for returning to the Air Force the decision-making power over its top programs.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A7546-2005Mar28.html>

7. *March 28, Government Accountability Office* — **GAO-05-182: Defense Acquisitions: Information for Congress on Performance of Major Programs Can Be More Complete, Timely, and Accessible (Report).** Department of Defense (DoD) has more than \$1 trillion worth of major defense acquisition programs, on which it must report to Congress, including a comparison of a current program's costs to a baseline containing its cost, quantity, schedule, and performance goals. When these goals are changed, the program is "rebaselined" to reflect

current status. However, measuring current estimates against the most recent baseline without additional perspectives may obscure for Congress how programs are performing over time. Concerned over this, Government Accountability Office (GAO) was asked to examine how DoD's use of rebaselining has affected the adequacy of data provided to Congress on major defense acquisition programs. To provide Congress with more complete, timely, and accessible information, GAO recommends that the Secretary of Defense implement the following changes: measure and report a full history of unit cost performance in constant dollars; notify Congress when a program is rebaselined; and separately report classified and unclassified data. DoD concurred with GAO's recommendations. Highlights:

<http://www.gao.gov/highlights/d05182high.pdf>

Source: <http://www.gao.gov/new.items/d05182.pdf>

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

Banking and Finance Sector

8. *March 29, ComputerWeekly* — **UK financial firms plan disaster simulation.** Banks and financial services companies in the UK are planning an exercise in November to test how they would respond to a major security incident in London. The exercise, which follows a smaller test at the end of last year, will assess the ability of UK firms to continue functioning following a major emergency. The test is being coordinated by the Bank of England, the Financial Services Authority and the UK Treasury as part of a three-way program to ensure the resilience of the financial sector. It is likely to be followed by a simulation of a terrorist attack on both sides of the Atlantic, in a collaboration between the UK, Canadian and U.S. governments.

Source: <http://www.computerweekly.com/articles/article.asp?liArticleID=137602&liArticleTypeID=1&liCategoryID=6&liChannelID=22&liFlavourID=1&sSearch=&nPage=1>

9. *March 29, eSecurityPlanet* — **Report finds banks careless with sensitive information.** The recent rash of personal data thefts may be keeping data brokers alert, but other industries could stand to improve their policies when it comes to keeping sensitive information secure, a new report finds. Financial services firms, retailers and insurance companies rated as the worst offenders in the loose-with-data category, according to a study released Monday, March 28, by Boston-based consulting firm The Customer Respect Group. Of the 60 financial services firms queried for the survey, including banks and brokerages, 43 percent admitted to sharing personal data with business partners or third parties. "It is not a good practice," said Terry Golesworthy, President of The Customer Respect Group. "If you look at the biggest fears of Internet users today, it is that there is too much personal information out there." Although the data intentionally leaked by companies in these industries is not of the same sensitive nature, for example, as the information divulged in the ChoicePoint debacle, e-mail address, zip codes and residential addresses are often used to cross-market products within their company, or even to third parties. Many times that data can lead to an influx of product pitches that many consumers don't like. Customer Respect Group: <http://www.customerrespect.com/>

Source: <http://www.esecurityplanet.com/trends/article.php/3493476>

10. *March 28, Associated Press* — **Stolen laptop exposes data of university students.** Someone recently walked into a University of California (UC), Berkeley office and stole a computer

laptop containing personal information on alumni, graduate students and past applicants. University officials waited until Monday, March 28, to announce the March 11 crime, hoping that police would be able to catch the thief and reclaim the computer. When that didn't happen, the school publicized the theft to comply with a state law requiring consumers be notified whenever their Social Security numbers or other sensitive information have been breached. UC Berkeley plans to advise the 98,369 people affected by the laptop theft to check their credit reports, although there has been no indication any of the personal information has been used illegally, university spokesperson Maria Felde said. The laptop stolen from the UC Berkeley was supposed to be encrypted this month, Felde said. The computer, which required a password to operate, was left unattended for a few minutes in a restricted area of a campus office before someone walked in and stole it, Felde said. Authorities suspect the thief was more interested in swiping a computer than people's identities.

Source: <http://www.securitypipeline.com/showArticle.jhtml?articleID=159907438>

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

Transportation Sector

11. *March 29, Reuters* — Delta to outsource maintenance work. Delta Air Lines Inc., which is facing a cash crunch, on Tuesday, March 29, said it expects to cut costs by about \$240 million over five years, becoming the latest airline to outsource aircraft maintenance work. Atlanta-based Delta said it will partner with Avborne of Miami, FL, and Air Canada Technical Services of Vancouver, Canada, to conduct heavy maintenance work on its aircraft fleet, cutting costs by 34 percent. Amid rising fuel prices and fare wars stemming from tough competition, several struggling U.S. airlines have outsourced maintenance work to cut costs, including UAL Corp.'s United Airlines, Northwest Airlines, Alaska Airlines and US Airways Group Inc. The parent of Air Canada, ACE Aviation Holdings Inc., on Tuesday said its contract to conduct heavy maintenance, repair and overhaul work on the Delta fleet would be worth \$300 million over five years. Delta also plans to reduce operations at its Tampa hangar, shifting some work to Atlanta. Tony Charaf, senior vice president of technical operations, outlined the planned savings in a memo to staff that was filed with the U.S. Securities and Exchange Commission. As previously announced, the division is slated to lose 1,600 to 2,000 jobs out of a total 6,000 to 7,000 job cuts.

Source: <http://www.reuters.com/newsArticle.jhtml?type=businessNews&storyID=8025843>

12. *March 29, Journal News (NY)* — Man tried to bring explosive cord on plane. A Stamford, CT, man was arrested at New York's Westchester County Airport on Monday, March 28, when he tried to board a plane with a piece of explosive detonating cord in his carry-on luggage, police said. Westchester County Public Safety Commissioner Thomas Belfiore said the man works for a company that sells explosive detection equipment and was on his way to St. Louis to demonstrate a piece of equipment. When a device used by baggage screeners indicated the presence of explosive material, they asked the man if he knew why. "He said, 'Oh, it's probably the explosive material in my bag,'" Belfiore said. "This prompted an interesting response on the part of the screeners and the police officers involved, to put it mildly." Frank Docimo, 50, was arrested on charges of third-degree criminal possession of a weapon and an unspecified violation of state labor law, both felonies. Belfiore said it appeared Docimo is legitimately employed by an international firm called Smith's Detection, which sells military and

nonmilitary detection equipment.

Source: <http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20050329/NEWS02/503290312/1023/NEWS07>

13. *March 28, Government Executive* — Citizen patrols on the Arizona border planned.

Recently, Jim Gilchrist, a California resident, put out a call for citizens to peacefully gather on the Arizona–Mexico border during April to monitor and report illegal immigration. Since then, more than 1,000 people, including 30 pilots with private aircraft, have pledged to set up camps along the border starting this Friday, April 1. Members of The Minuteman Project, as it is called, say their goal is to draw attention to illegal immigration and gaps in border security, while helping to secure the areas they monitor. Participants pledge not to make contact with illegal immigrants, only watch and report their activities to the Border Patrol. The main area of observation will be a 20–mile stretch of lowlands across the San Pedro Valley in Southeast Arizona. Estimates on the number of illegal immigrants in the country range from eight million to 20 million, the vast majority of whom enter through the Southwest border. T.J. Bonner, president of the American Federation of Government Employees' National Border Patrol Council, estimates that the Border Patrol catches only between a quarter and a third of all illegal crossers. "We're just overwhelmed," Bonner said. For further information:

<http://www.minutemanproject.com/>

Source: <http://www.govexec.com/dailyfed/0305/032805c1.htm>

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

14. *March 29, Capital Press Agriculture Weekly (OR)* — California's bovine tuberculosis status could change. Cattle could move a little more easily across the state border later this year if California's bovine tuberculosis (TB) status is upgraded. Since no new cases of the disease have been found since the last infected dairy herd was depopulated two years ago, the state has asked the U.S. Department of Agriculture to upgrade its status, effective April 30. Since the contagious disease was found in three dairy herds in Tulare, Kings, and Fresno counties in 2002, the state has tested more than 875,000 animals for bovine TB. Since that time, officials have not found any additional infections, but had been able to trace the source of the disease back to cattle that were imported from out of state. In its effort to eradicate the disease, state officials tested a total of 688 dairy herds and destroyed about 13,000 cattle. Since the disease was found in California, cattle producers have been required to test most cattle for TB before moving them across the state line. In addition, individual states across the nation have imposed their own TB–testing requirements on top of what the federal government has required.

Source: <http://www.capitalpress.info/Main.asp?SectionID=67&SubSectionID=792&ArticleID=16184>

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

Food Sector

Nothing to report.

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

Water Sector

15. *March 30, Monterey County Herald (CA)* — **Army officials investigate water contamination near Fort Ord.** The U.S. Army is expanding an investigation into the size of a toxic groundwater plume after discovering trichloroethene (TCE) contamination in shallow test wells between Fort Ord, CA, and Armstrong Ranch to the north. The contaminant was previously identified in wells southeast of the Fort Ord, but the new discovery indicates the contamination may be migrating west. The location of the contamination is in the shallow aquifer, about 100 feet from the surface. The drinking wells that supply Fort Ord draw water from 200 to 400 feet beneath the surface, and Marina Coast Water District's wells pump water from a depth of about 900 feet, so according to Gail Youngblood, the Army's Base Realignment and Closure environmental coordinator, the well water is not in danger. The extent of the plume that has been identified to date is about 1½ miles from the coast, Youngblood said. The source of the plume is an area that was used as a fire drill site near the former Fritzsche Army Airfield, now the Marina Coast Municipal Airport. In the 1950s, the earthen dam was filled with flammable chemicals and lit for Army firefighting practice. Additional information:

<http://www.fortordcleanup.com/>

Source: <http://www.montereyherald.com/mld/montereyherald/news/local/11256920.htm>

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

Public Health Sector

16. *March 29, Reuters* — **Vietnam family of five confirmed with bird flu.** A Vietnamese couple and their three children have been infected by bird flu in the latest human cases of the virus which has killed 49 people since the end of 2003, state media reported on Tuesday, March 29. The five, from a district where bird flu had killed poultry, were sent to hospital in the northern port of Haiphong last week suffering fevers and breathing problems. Preliminary tests on the 39-year-old man, his wife and their three daughters — aged between four months and 10 years — confirmed they had the H5N1 variant of the virus, the Lao Dong newspaper reported.

Source: <http://www.reuters.com/newsArticle.jhtml?type=healthNews&storyID=8018392>

17. *March 29, Canadian Press* — **Congolese official fears Marburg virus will cross border from Angola.** The Republic of Congo's top health official said Monday, March 28, he fears an outbreak of a rare hemorrhagic fever could spread from neighboring Angola despite efforts to curtail cross-border traffic and monitor arrivals from the infected area. Damase Bozongo, director general for health, told The Associated Press that he did not understand why Angolan officials do not quarantine the border area affected by the Marburg virus, which has killed at least 112 people. In January, he said, long before the illness was identified as Marburg, Congo

sent a medical team to the border to monitor and counsel people living near the frontier between the two countries share. Officials have been asked to carefully check people arriving from Angola and rush to the hospital any suspect cases arriving at Pointe-Noire, Congo's petroleum port that has a well-traveled road to Angola's affected Uige province and daily flights from Luanda, the Angolan capital. Additional information is available from the Centers for Disease Control and Prevention:

<http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/marburg.htm>

Source: <http://www.canada.com/health/story.html?id=bba78d93-dae5-4af9-a5af-eb398c57dbe1>

18. *March 02, Clinical Infectious Diseases* — Purpura fulminans due to Staphylococcus aureus.

Purpura fulminans is an acute illness commonly associated with meningococemia or invasive streptococcal disease. Researchers report the first five cases (to their knowledge) of purpura fulminans directly associated with Staphylococcus aureus strains that produce high levels of the superantigens toxic shock syndrome toxin 1 (TSST-1), staphylococcal enterotoxin serotype B (SEB), or staphylococcal enterotoxin serotype C (SEC). Cases were identified in the Minneapolis, MN, area during 2000–2004. S. aureus infection was diagnosed on the basis of culture results. The ability of the isolated organisms to produce TSST-1, SEB, SEC, and Pantan–Valentine leukocidin (PVL) was determined. In three of the five cases, the infecting S. aureus strain was isolated from the blood cultures. In two of the five cases, the infecting S. aureus strain was isolated only from the respiratory tract, indicating that purpura fulminans and toxic shock syndrome resulted from exotoxin and/or other host factors, rather than septicemia. One of these latter two patients also had necrotizing pneumonia, and the isolated S. aureus was a methicillin-resistant strain that produced both SEC and PVL. Staphylococcal purpura fulminans may be a newly emerging illness associated with superantigen production. Medical practitioners should be aware of this illness.

Source: <http://www.journals.uchicago.edu/CID/journal/issues/v40n7/34613/brief/34613.abstract.html>

19. *February 15, PLoS Medicine* — Researchers propose space–time permutation scan statistic for disease outbreak detection.

The ability to detect disease outbreaks early is important in order to minimize morbidity and mortality through timely implementation of disease prevention and control measures. Many national, state, and local health departments are launching disease surveillance systems with daily analyses of hospital emergency department visits, ambulance dispatch calls, or pharmacy sales for which population-at-risk information is unavailable or irrelevant. Researchers propose a prospective space–time permutation scan statistic for the early detection of disease outbreaks that uses only case numbers, with no need for population-at-risk data. It makes minimal assumptions about the time, geographical location, or size of the outbreak, and it adjusts for natural purely spatial and purely temporal variation. The new method was evaluated using daily analyses of hospital emergency department visits in New York City. Four of the five strongest signals were likely local precursors to citywide outbreaks due to rotavirus, norovirus, and influenza. The number of false signals was at most modest. If such results hold up over longer study times and in other locations, the space–time permutation scan statistic will be an important tool for local and national health departments that are setting up early disease detection surveillance systems.

Source: <http://medicine.plosjournals.org/perlserv/?request=get-document&doi=10.1371/journal.pmed.0020059>

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

Government Sector

Nothing to report.

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

Emergency Services Sector

20. *March 29, The Star-Ledger (NJ)* — **New Jersey state police to aid threatened public officials via Website.** The New Jersey State Police unit that investigates threats against judges and lawmakers is launching a new system to help it respond quickly to signs of trouble and avoid tragedies like those that recently struck Chicago and Atlanta. A new, secure Website set to debut in a few weeks will allow officials who receive threats to report them immediately to the State Police central security unit, and enable the police to quickly spread warnings of any general threats against public officials. The site also will have directions for officials and their staffs to follow when they receive threats. The State Police last year investigated about 120 threats against lawmakers, judges and their staffs. Increasingly, those threats are being made over the Internet via e-mail or state Websites. State Police and the Office of Legislative Services began working several months ago to develop an Intranet site that would allow police and officials to communicate directly about threats made in person, through the mail, over the Internet or by telephone. The plan is to put an icon on each office's home page that will link directly to the threat management Intranet site. New Jersey State Police Website:
<http://www.njsp.org/>
Source: <http://www.nj.com/news/ledger/jersey/index.ssf?/base/news-9/1112079321135130.xml>

21. *March 29, Des Moines Register ((IA)* — **Statewide tornado drill scheduled in Iowa.** Area residents will be reminded of the upcoming severe weather season when public safety officials hold a tornado drill Wednesday, March 30. Plans call for a mock tornado watch to be issued around 10 a.m., followed by a tornado warning. The statewide drill is expected to end around 10:30 a.m. If there is severe weather Wednesday, the test will be delayed until Thursday. David Burns, Ankeny's fire chief and director of emergency management, said the drill is a good opportunity for residents to become more familiar with severe weather safety. In addition to local public safety officials, Ankeny's Community Emergency Response Team will take part in Wednesday's tornado drill. Organization members are participating in training and other activities to form a severe weather spotters' group for the Ankeny area. Officials have compiled a list of suggestions residents can use to protect themselves during severe weather. Residents are also encouraged to put together an emergency storm kit that includes candles, matches, a transistor radio, flashlight and batteries, and simple first aid items in a waterproof container.
Source: <http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20050329/NEWS02/503290317/1004>

22. *March 27, Stars and Stripes* — **Mass-casualty drill tests emergency preparedness of Marines on Okinawa.** “Terrorists” struck Camp Schwab on Okinawa, Japan, on Thursday,

March 24, as a dirty bomb was set off, “killing” several Marines and “injuring” dozens more. But that wasn’t the only incident that day: a nerve agent was released in the air vents of a Camp Courtney barracks, doing damage to even more Marines. The mass-casualty drill was the major event of an annual weeklong force-protection exercise the U.S. Marines were holding. Other events throughout the week included various heightened force-protection measures and testing of security forces and first responders on proper manning and response procedures. The exercise is designed to “ensure that we have a safer environment in which our personnel, employees and family members can live and conduct their missions,” according to a Marine Corps Base public affairs spokesperson. About 1,000 Marines, soldiers, sailors and airmen took part in the exercise. “Drills like this keep everyone refreshed on the emergency process,” said Navy Capt. Rick Becker, Naval Hospital commanding officer. “This helps us find where our fail points are...so we can improve on them.”

Source: <http://www.estripes.com/article.asp?section=104&article=27128&archive=true>

23. *March 26, News-Leader (MO)* — **Bioterror drill in Missouri deemed success.** Last April, local agencies testing their response to a simulated bioterror attack in downtown Springfield, MO, pinpointed two areas of improvement: communication and coordination. On Thursday, March 24, more than 120 people on the Springfield-Greene County homeland security team participated in a full-scale exercise aimed at disarming a simulated terrorist threat west of Springfield. The fictional scenario involved five militants from the Ozarks who had hijacked two tankers filled with hazardous chemicals and were plotting to use them as weapons of mass destruction. David Hoover, who evaluated the response of CoxHealth emergency medical services during the drill, was pleased with what he saw Thursday. Medical technicians who participated in the training exercise properly decontaminated, triaged and treated the two terrorists exposed to chemicals during the shootout, said Hoover. "One of the things that went really well was that they didn't go running into a dangerous situation," he added. Evaluators who graded the team's response met Friday morning to solidify their comments and critiques about Thursday's exercise, said Larry Woods, assistant director of the Springfield-Greene County Emergency Management Office.

Source: http://springfield.news-leader.com/news/today/20050326-Terro_rdrilldeem.html

[[Return to top](#)]

Information Technology and Telecommunications Sector

24. *March 29, Secunia* — **EncapsBB "root" file inclusion vulnerability.** A vulnerability in has been reported in EncapsBB, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "root" parameter in "index_header.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. There is no solution at this time.

Source: <http://secunia.com/advisories/14761/>

25. *March 29, Secunia* — **Smail-3 "Mail From" buffer overflow and signal handling vulnerabilities.** Some vulnerabilities in Smail-3, which potentially can be exploited by malicious, local users to gain escalated privileges and by malicious people to compromise a vulnerable system. A boundary error within the SMTP server when handling email addresses

can be exploited to cause a heap-based buffer overflow by passing an overly long string to the "MAIL FROM" command. Some design errors exist within the signal handling code. This may potentially be exploited by malicious, local users to execute arbitrary code with escalated privileges. There is no solution at this time.

Source: <http://secunia.com/advisories/14733/>

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: US-CERT has identified a recent increase of reported P2P incidents. P2P file sharing technology provides Internet users with the potential to share local files with a potentially unlimited number of other Internet users. As a result, the usage of P2P software may allow for sensitive data or personal information to be leaked from computer systems. Further, P2P may provide a vector for malicious code to be introduced into an enterprise environment.

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 22321 (wnn6_Tw), 135 (epmap), 1025 (----), 80 (www), 139 (netbios-ssn), 53 (domain), 1026 (----), 7674 (----), 1027 (icq)
----------------------------	---

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.