



# Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 28 February 2005

Current  
Nationwide  
Threat Level is  
**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS  
[For info click here](http://www.dhs.gov/)  
<http://www.dhs.gov/>

## Daily Highlights

- CNET News reports the Bank of America has lost backup tapes with records detailing the financial information of possibly 1.2 million SmartPay charge card customer records. (See item [6](#))
- CNET News reports online payroll service provider PayMaxx closed its automated W-2 site after a researcher claimed that two security holes could allow anyone to view the W-2 forms generated for employees of PayMaxx's clients for the last five years. (See item [7](#))
- The Associated Press reports patrols have been stepped up around the Detroit Metropolitan Airport after two Northwest Airlines pilots reported that laser lights were shined into their cockpits as they were about to land their planes. (See item [8](#))

### DHS/IAIP Update *Fast Jump*

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

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

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

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

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

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

## Energy Sector

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

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

1. *February 26, CBS MarketWatch* — **Oil price surge defies forecasters.** As crude-oil futures climbed above \$51 a barrel recently, analysts threw up their hands and wondered why. "None of the historical correlations analysts have used — inventories primarily for oil, storage for natural gas, natural-gas and oil prices for rig counts — work," said Jim Wicklund, managing director of energy research at Banc of America Securities. "No one can really explain, with

anything but a very broad brush, why crude oil prices are as high as they are." Pointing to the Department of Energy and American Petroleum weekly U.S. inventory reports, James Williams, an energy economist at WTRG Economics, said nothing in the data supports prices at this level. One reason for the disparity between forecasts and the current price of crude is a bias on the part of analysts. Most analysts believe that oil will return to normal levels, though he said there's no longer a good way to gauge what is normal. Secondly, demand from China has skyrocketed. Thirdly, in some areas of the world, supply growth has hit a wall.

Source: <http://www.marketwatch.com/news/yhoo/story.asp?source=blq/yhoo&siteid=yhoo&dist=yhoo&guid=%7B26A99421%2D6173%2D418C%2D8E53%2D37C92691BF52%7D>

- 2. February 25, Department of Energy — Government officials from United States, Canada and Mexico release natural gas report.** The North American Energy Working Group (NAEWG), a group of senior energy officials from Canada, Mexico and the United States, on Friday, February 25, released the "North American Natural Gas Vision," a trilateral report by the three governments that includes information on the natural gas market in the North American region, including forecasts through the year 2012. The "North American Natural Gas Vision" contains three sections: a summary of key findings; a review of the sector from 1990 to 2003; and a forecast on market supply, demand, prices, and trade out to the year 2012. The report also includes comments on issues beyond 2012. The report is the culmination of two years' work by the NAEWG's Natural Gas Experts Group, which reviewed various measures North America can take to achieve its goals for natural gas. It examines the increasingly important role of natural gas in the energy sectors of the three countries and will serve as an important reference document for governments, businesses and the general public. Report: <http://www.pi.energy.gov/pdf/library/NAEWGGasVision2005.pdf>  
Source: [http://www.energy.gov/engine/content.do?PUBLIC\\_ID=17526&BT\\_CODE=PR\\_PRESSRELEASES&TT\\_CODE=PRESSRELEASE](http://www.energy.gov/engine/content.do?PUBLIC_ID=17526&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE)

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

## **Chemical Industry and Hazardous Materials Sector**

- 3. February 27, Associated Press — Hundreds evacuated after chemical leak.** Up to 400 people were evacuated from their homes Saturday, February 26, after corrosive chemicals leaked from a tanker truck in the rural neighborhood of Pedley, CA, sending a plume of toxic gas into the sky. Firefighters went door to door ordering neighbors out of their homes, after more than 200 gallons of the unidentified chemical spilled onto the ground while the truck was parked in a driveway. No injuries were reported. The gas plume was believed to be hazardous, so cleanup crews wore protective suits while police remained upwind from the spill. Officials believe the substance was some type of acid or mix of corrosive chemicals, Riverside County Fire Captain Rick Vogt said.  
Source: <http://www.wtlv.com/news/news-article.aspx?storyid=33162>
- 4. February 27, Daily Local News (PA) — Study to target Hazmat cargo.** Authorities estimate that five truckloads of hazardous materials travel on Chester County, PA, roads each hour, according to a 1994 study. And each of those truckloads, by very definition, poses a risk to the county's 433,000 residents. Thanks to a grant from the U.S. Department of Transportation, the

Chester County Department of Emergency Services will be able to update those statistics when a new study is completed in 2005. The Commodity Flow Study will show what substances are traveling on which roadways at any given time, allowing emergency responders to gain awareness of what potential problems could occur and where. The focus will be on the major corridors in the county that see interstate or regional truck traffic.

Source: [http://www.zwire.com/site/news.cfm?newsid=14044710&BRD=1671&PAG=461&dept\\_id=17782&rfti=6](http://www.zwire.com/site/news.cfm?newsid=14044710&BRD=1671&PAG=461&dept_id=17782&rfti=6)

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

## **Defense Industrial Base Sector**

Nothing to report.

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

## **Banking and Finance Sector**

5. *February 25, BBC News (UK)* — **Online commerce affected by phishing.** Fake bank e-mails, or phishing, and stories about identity theft are damaging the potential of using the net for online commerce, say e-business experts. Trust in online security is falling as a result. Almost 70% of those asked in a poll said that net firms are not doing enough to protect people. The survey of more than 1,000 people reported that 43% were not willing to hand over personal information online. More people are becoming aware of online security issues but they have little confidence that companies are doing enough to counter the threats, said security firm RSA, which carried out the poll. Security experts say that scare stories and the vulnerabilities dogging e-commerce and e-banking are being taken seriously — by banks in particular. Many believe using login details like usernames and passwords are simply not good enough anymore though. One of the biggest challenges to improving security online is how to authenticate an individual's identity.

Source: <http://news.bbc.co.uk/1/hi/technology/4273135.stm>

6. *February 25, CNET News* — **Bank of America loses customer records.** Backup tapes with records detailing the financial information of government employees were lost in shipment to a backup center, Bank of America said on Friday, February 25. The tapes contained information on the customers and accounts of the U.S. government's SmartPay charge card program, which has more than 2.1 million members and annual transactions totaling more than \$21 billion, according to the General Services Administration. Reports have pegged the number of cards affected at 1.2 million. Federal law enforcement officials were immediately engaged when the tapes were discovered missing, and subsequently conducted a thorough investigation into the matter, working closely with Bank of America," the bank said in a statement. "The investigation to date has found no evidence to suggest the tapes or their content have been accessed or misused, and the tapes are now presumed lost." Bank of America said it will continue to monitor the accounts on the data tapes and will contact the government cardholders if any unusual activity is observed.

Source: [http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029\\_3-5590989.html](http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html)

7. *February 23, CNET News* — **Payroll site closes on security worries.** Online payroll service provider PayMaxx closed its automated W-2 site on Wednesday, February 23, after a researcher claimed that two security holes had exposed data on more than 25,000 people. A description of the problem posted on Think Computer's Website by Aaron Greenspan, president of the software start-up, said the security issues could allow anyone to view the W-2 forms generated for employees of PayMaxx's clients for the last five years. PayMaxx did not acknowledge or deny the problems, saying that a third-party security company was investigating the allegations. Greenspan, a former PayMaxx customer, said he discovered the alleged problems in the company's system more than two weeks ago, after he received notification from the company that his W-2 tax form was available online for download and printing. The link to access the W-2 included an ID number, and he wondered whether the company had protected against an obvious security problem: adding one to the ID number to get the next form. Instead of being denied access, Greenspan found that another person's W-2 was downloaded and readable. PayMaxx declined to comment on whether it had notified any of its customers about the problem.

Source: [http://news.com.com/Payroll+site+closes+on+security+worries/2100-1029\\_3-5587859.html](http://news.com.com/Payroll+site+closes+on+security+worries/2100-1029_3-5587859.html)

[[Return to top](#)]

## **Transportation Sector**

8. *February 27, Associated Press* — **Patrols stepped up at Detroit airport after laser reports.** Patrols have been stepped up around Detroit Metropolitan Airport after two Northwest Airlines pilots reported last week that laser lights were shined into their cockpits as they were about to land their planes. Laser lights were shined at the planes from an area along Interstate 94 just east of the airport on Thursday night, February 24. Neither entered the cockpit or affected the landing of the jets, airport officials said. Over the past four months, the FAA has received dozens of reports of lasers being pointed at airplanes in several states. Shining a laser at a plane can be considered a 20-year federal felony of interfering with flight crews.
9. *February 25, Associated Press* — **Commuter train catches fire in Chicago.** An elevated train filled with passengers on their morning commute caught fire Thursday, February 24, and the conductor was forced to make two emergency stops before all the riders could be evacuated. No injuries were reported, but several passengers were trapped on the train as it drove about a half mile to a second station while two middle cars burned. The train finally pulled onto empty tracks, where flames blackened two of its cars and warped window frames. The train operator spotted smoke while pulling out of the 43rd Street station and made an emergency stop, but only the last three cars of the six-car train were still in the station where the passengers could get out, Chicago Transit Authority spokesperson Robyn Ziegler said. The cause of the fire wasn't immediately clear.

Source: [http://www.usatoday.com/news/nation/2005-02-24-train-fire\\_x.htm](http://www.usatoday.com/news/nation/2005-02-24-train-fire_x.htm)

10. *February 24, New York Times* — **FAA wants upgraded cockpit voice recorders.** The Federal Aviation Administration (FAA) proposed a rule on Thursday, February 24, that would require

airlines to install cockpit voice recorders with two hours of recording time and a backup power source. The agency stopped short of proposing video cameras, which crash investigators are urging. The changes would cost about \$256 million and include equipment for newly built planes as well as about 9,600 commercial planes already flying. Airlines, some bankrupt and some close to it, are likely to file objections in the next two months to a draft rule that has been published for public comment. Most cockpit voice recorders use either tape or computer data storage chips. The proposal would require chips because they are more likely to survive a crash. The new recorders would also have to handle two hours of information, including voices and cockpit sounds, rather than 15 to 30 minutes as they do now. The proposed rule would also require changes to the other "black box," the flight data recorder, but only on new planes. The Federal Aviation Administration was responding to recommendations made by the National Transportation Safety Board, an advisory agency that is in charge of crash investigations.

Source: <http://www.nytimes.com/2005/02/25/politics/25recorder.html?pagewanted=all&oref=login>

11. **February 24, *United Press International* — U.S. wants passenger names one hour before takeoff.** The Department of Homeland Security is drafting a rule that will require airlines to pass on passenger manifest information as much as an hour before the departure of international flights bound for the United States, officials confirmed on Thursday, February 24. "We need to be able to identify any suspected terrorists or other criminals (on board) before the plane takes off," Christiana Halsey of the department's Customs and Border Protection directorate said. Halsey said that the passenger names would, as at present, be checked by the directorate's National Targeting Center against the United States' consolidated terrorist watchlist — which contains the names and aliases of thousands individuals thought linked to terrorism — and against several other law-enforcement databases. "We're not just looking for terrorists," she said. All that would change is that airlines would have to submit the data up to one hour before the plane takes off, rather than within 15 minutes of departure under current procedures. Industry sources said the move could create serious logistical problems for airlines, which currently do not finalize their passenger manifests until the doors of the plane close at the gate as the plane departs.

Source: <http://www.upi.com/view.cfm?StoryID=20050224-105943-7064r>

12. **February 24, *Transportation Security Administration* — Explosives detection trace portals installed at Las Vegas Airport.** The Transportation Security Administration (TSA) on Thursday, February 24, announced the installation of two explosives detection trace portals at checkpoints C and D in McCarran International Airport's Terminal 1. The airport will be the ninth in the nation to receive the portals and the first to receive more than one. The equipment is part of Phase II of a pilot program to test and evaluate the equipment for explosives screening of passengers. The portals detect explosives by blowing several "puffs" of air onto passengers. Air samples are then collected and analyzed for explosives. If the portal alarms, passengers go through additional screening. If the portal does not alarm, a computerized voice tells the passenger to continue the screening process. By testing two trace portals at McCarran, TSA will be able to evaluate electrical and other logistical requirements in an airport setting while collecting data on security and customer service impacts.

Source: [http://www.tsa.gov/public/display?theme=44&content=090005198\\_01034c0](http://www.tsa.gov/public/display?theme=44&content=090005198_01034c0)

13.

**February 24, GovExec — New passenger screening system expected to begin in August.**

The Transportation Security Administration (TSA) expects to begin using a new computer system to prescreen airline passengers this summer, an agency spokesperson said on Thursday, February 24. TSA plans to issue a regulation giving it the power to check passengers flying on two of the nation's air carriers against expanded government no-fly and terrorist watch lists starting in August, said TSA spokesperson Amy Von Walter. The agency has not decided yet which carriers will be selected. The system, called Secure Flight, is intended to check personal information on everyone who flies within the United States against watch lists of known or suspected terrorists at the FBI's Terrorist Screening Center, including expanded no-fly and selectee lists. Information that might be checked could include a passenger's name, reservation date, travel agency or agent, travel itinerary, form of payment, flight number and seating location. TSA plans two phases of testing to determine the cost, feasibility and effectiveness of using commercial data. The tests are scheduled to begin in late February or early March, with results expected in April.

Source: <http://www.govexec.com/dailyfed/0205/022405c1.htm>

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

## **Postal and Shipping Sector**

14. **February 26, News-Times (CT) — Envelope with white powder sent to prosecutor.** An office at the Danbury, CT, Superior Court was evacuated Friday, February 25, after a secretary opened an envelope believed to be from an inmate and a white, powdery substance fell out. The white powder, which courthouse sources feared could be anthrax, was inside a letter sent to the State's Attorney Office on the first floor of the White Street building, state police said. There was some indication the letter was sent by a prisoner in a correctional facility, police said. Everyone who worked in the state's attorney's office was evacuated after the 2 p.m. incident, said Melissa Farley, of the state Judicial Branch. "The letter was being bagged and it's being tested," Farley said. The rest of the courthouse remained staffed and visitors were allowed to come and go until 4 p.m., when court officials began screening visitors, allowing the public in only for urgent business.

Source: <http://news.newstimes.com/story.php?id=69391&channel=Local>

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

## **Agriculture Sector**

15. **February 26, Associated Press — Mad cow case confirmed in Japan.** Japan has confirmed its 15th case of mad cow disease, the Japanese government said Saturday, February 26. The 102-month-old cow from a ranch in northern Hokkaido prefecture has tested positive for the fatal brain-wasting disease, the Agriculture Ministry said in a statement. The finding confirms the results from preliminary tests conducted on the animal earlier this week.

Source: <http://cnews.canoe.ca/CNEWS/World/2005/02/25/942864-ap.html>

16. **February 25, USAgNet — Beekeeping industry impacted by parasite.** The Varroa mite, an exotic Asian parasitic insect attacking Honeybee larvae in their hives, has been marching

almost unchecked across the landscape of U.S. agriculture. Many beekeepers have reported that Varroa destructor has wiped out 50 percent or more of their cultivated hives. The mite has also attacked feral populations of Honeybees in virtually every state in the U.S. One of every three bites of food consumed in the U.S. comes from crops pollinated by Honeybees. While some plant and tree yields are merely helped by Honeybee pollination, other crops must have pollination in order to have any yield at all. Research projects are currently being funded at universities and bee research laboratories and new research positions have been created in fields as diverse as molecular biology, ecology, pollination, and toxicology, all with the intention of eradicating the Varroa mite.

Source: <http://www.usagnet.com/story-national.cfm?Id=219&yr=2005>

17. *February 25, Pioneer Press (MN)* — **Wisconsin deer tests positive for chronic wasting disease.** A deer shot and killed by a hunter in Walworth, WI, has tested positive for chronic wasting disease (CWD), the Department of Natural Resources says. The agency said Wednesday, February 23, that the buck, about 18 months old, was shot by a hunter north of Lake Geneva. It said the deer was the 11th in the county confirmed to have the disease and was farther to the east than any of the others. Besides Walworth County, deer have also tested positive for the disease in Columbia, Dane, Green, Iowa, Kenosha, Richland, Rock, and Sauk counties.

Source: <http://www.twincities.com/mld/pioneerpress/news/local/109852.85.htm?1c>

18. *February 24, Farm Week (IL)* — **Sustained rust resistance issue for Brazilian breeders.** In an attempt to control an Asian soybean rust, Brazilian researchers are working to build a genetic arsenal that will allow farmers to continue a long-term fight against the disease. Rust presents a special challenge because of its high degree of variability — it can develop several races within a short period — and high spore dispersal capacity. To date, Brazil’s Embrapa soy research center has identified several highly tolerant soy breeding lines. But because of rust’s variability, researchers also are studying genes that provide lesser levels of tolerance but could bolster basic resistance traits. One variety now in final yield trials has shown continued resistance and should be available in another year for use in central Brazil. But Jose Francisco Ferraz de Toledo, a scientist with Embrapa, noted several promising resistant genes are now susceptible to rust. Toledo reported, “we cross just about everything with everything in the program,” in search of materials with added tolerance or that may slow or delay the disease cycle, thus allowing farmers to “escape with just one (fungicide) spraying.” Though Embrapa focuses on varieties suited to Brazil’s specific agronomic conditions, breeder Paul Stephens noted “the genes will transfer,” opening the door to biotech rust solutions.

Source: <http://farmweek.ilfb.org/viewdocument.asp?did=7634&drvid=105 &r=0.7909662>

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

## **Food Sector**

Nothing to report.

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

## **Water Sector**

19. *February 25, Arizona Republic* — **Arizona's Roosevelt Lake rebounding after nine year drought.** Arizona's Roosevelt Lake will reach historically high levels Friday, February 25, and likely will fill to capacity by spring. News of the high levels comes just three years after the giant reservoir nearly dried up. The swelling of the lake can be attributed to runoff from a series of winter storms that have more than doubled the lake's size in the past 55 days. As a result, the valley area's water supply is in its best shape in more than a decade. The Salt River Project, which manages Roosevelt and five other reservoirs, will head into the warm-weather months with a nearly full system for the first time since the early 1990s, allowing the utility to stop tapping backup wells. Six valley cities will reap these benefits as runoff into Roosevelt fills new storage space created by the enlarged dam. Those cities include Phoenix, Mesa, Glendale, Scottsdale, Tempe and Chandler.

Source: <http://www.azcentral.com/arizonarepublic/news/articles/0225roosevelt25.html>

20. *February 25, The Record (CA)* — **California agency votes to loosen rules on toxic waterway releases.** California state water-pollution officials voted Thursday, February 24, to ease rules that control how toxic metals are discharged into waterways, ruling despite objections from several federal agencies, Central Valley regulators, environmentalists, and a California trade association. Toxic metals are a concern in California because a number of fish species as well as the plankton they eat are in decline. Even very low levels of metals such as copper and nickel can kill aquatic life. Before the rule changes can go into effect, they must be reviewed by California's Office of Administrative Law and then win approval from the federal Environmental Protection Agency. The rule changes were designed to make life easier for those who operate sewage-treatment plants, because according to sewage-plant operator representatives, the old rule forced plant operators to do excessive monitoring. Right now, California sets limits for pollutants based on how water is used. A river that is used for farm irrigation, to support fish, and for drinking would have pollution limits that protect all those uses.

Source: <http://www.recordnet.com/daily/news/articles/022505-gn-8.php>

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

## **Public Health Sector**

21. *February 27, Associated Press* — **Vietnam confirms another bird flu death.** Vietnamese officials confirmed on Sunday, February 27, that a 69-year-old man has died from bird flu, the 14th person to die from the disease this year. The man, from northern Thai Binh province, was admitted to the provincial hospital on February 19 with symptoms of high fever and breathing difficulties, said Pham Van Diu, director of Thai Binh Provincial Preventive Medicine Center. Samples taken from the man, who died on Wednesday, February 23, tested positive for the H5N1 virus, Diu said. Relatives of the latest victim said his whole family had eaten chicken, a traditional dish, during Lunar New Year festivities earlier this month, Diu said. None of them have reported any illness. On Friday, February 25, Vietnam had reported that a 21-year-old man from the same province had tested positive for bird flu. Initial tests on his 14-year-old sister, who was also suspected of having contracted the virus, have come up negative.

Source: <http://abcnews.go.com/Health/wireStory?id=535500>

22. *February 26, Lancet* — **Assessment of influenza vaccines in children.** Researchers assessed evidence of efficacy and effectiveness of live attenuated and inactivated influenza vaccines in children up to 16 years of age. Researchers searched the Cochrane Library, MEDLINE, EMBASE Biological Abstracts, and Science Citation Index to June 2004, in any language, and contacted vaccine manufacturers and authors of relevant studies to identify additional data. Live attenuated influenza vaccines had 79 percent efficacy and 38 percent effectiveness in children older than two years compared with placebo or no immunization. Inactivated vaccines had lower efficacy — 65 percent — than live attenuated vaccines, and in children aged two years or younger they had similar effects to placebo. Effectiveness of inactivated vaccines was about 28 percent in children older than two years. Studies assessing the effects of vaccines against secondary cases suggested no difference with placebo or standard care. Influenza vaccines (especially two-dose live attenuated vaccines) are efficacious in children older than two years. Efficacy and effectiveness of the vaccines differed strikingly. If influenza immunization in children is to be recommended as public-health policy, large-scale studies assessing such important outcomes and undertaking direct comparisons of vaccines are urgently needed. Source: <http://www.thelancet.com/journal/journal.isa>

23. *February 25, Reuters* — **Ethiopia records polio case as virus spreads.** A two-year-old girl has contracted polio in Ethiopia in another sign that the epidemic is spreading across Africa, the World Health Organization (WHO) said on Friday, February 25. It was the 14th previously polio-free country to record an imported case, including 13 in Africa, posing a fresh setback to the United Nations campaign to halt transmission of the crippling virus by year-end. WHO officials say the virus originated in Nigeria 18 months ago, after the northern state of Kano suspended vaccinations, and has traveled east as far as Sudan and Saudi Arabia. "The (Eritrean) Ministry of Health team has reported back that they have seen the first case and are looking at another suspect case today," Bruce Aylward, coordinator of the WHO's global polio eradication initiative, told a news briefing. Source: <http://www.reuters.com/newsArticle.jhtml?type=healthNews&storyID=7740126>

24. *February 25, New York Times* — **Two new viruses reported belonging to AIDS family.** Scientists said Friday, February 25, that they had discovered two new human viruses in Africa that belong to the same family, retroviruses, as the virus that causes AIDS. So far, the scientists said, the new viruses have not been linked to any disease, but they are being monitored out of concern that they or similar retroviruses might conceivably spawn another epidemic. The viruses, found in rural Cameroon among people who hunt monkeys and other primates, were probably transmitted from the animals through blood from bites and scratches received in hunting, butchering, and keeping the primates as pets, the scientists said at the 12th Annual Retrovirus Conference. One scientist who discovered the new viruses in Africa, Walid Heneine, a virologist at the U.S. Centers for Disease Control and Prevention, said his team was expanding its research to determine the health status of the infected people and of their sexual partners. The team is conducting additional tests to identify other novel viruses. The studies show that "there is frequent ongoing transmission" from nonhuman primates, Heneine told reporters. The retroviruses, named HTLV-3 and HTLV-4, for human T-lymphotropic virus, are the newest members of a class that can cause a wide spectrum of illnesses. Source: <http://www.nytimes.com/2005/02/26/national/26aids.html>

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

## Government Sector

Nothing to report.

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

## Emergency Services Sector

### **25. *February 25, New Britain Herald (CT)* — Firefighters training as first responders.**

Firefighters in New Britain, CT, will be riding with New Britain Emergency Medical Service (EMS) personnel during the next two weeks to better prepare themselves to work as first responders. Bruce Baxter, director of the New Britain EMS, said he expected the Fire Department, once it takes on responsibilities of responding to some 911 calls, to be on the scene at as many as 4,000 of the 11,000 emergency calls fielded per year. Firefighters will respond to most calls categorized as life-threatening emergencies, to which a speedy response is essential to survival, Baxter said. EMS ambulances will still be transporting the patients to area hospitals, but firefighters will be able to be on scene earlier to administer medical treatment, he said. Four firefighters will be rotating through the EMS facility every four hours for 16 hours a day until all the firefighters have spent time responding to emergency calls with the emergency medical personnel.

Source: [http://www.newbritainherald.com/site/news.cfm?newsid=14033140&BRD=1641&PAG=461&dept\\_id=10110&rfi=6](http://www.newbritainherald.com/site/news.cfm?newsid=14033140&BRD=1641&PAG=461&dept_id=10110&rfi=6)

### **26. *February 24, Government Technology* — Grants to upgrade Virginia's first responder radio systems announced.**

Virginia Governor Mark R. Warner announced on February 23 that the state is allocating \$2.16 million in federal funding to 27 localities to support local interoperable communications projects and initiatives. The State Interoperability Executive Committee evaluated 62 local grant proposals that competed for up to \$100,000 each, which includes 20 grant proposals that will be funded through a \$1.7 million award from the federal Office of Domestic Preparedness. Additionally, three demonstration projects were funded by the award from the National Institute of Justice. Stafford County, King George County, and the cities of Spotsylvania and Fredericksburg will receive \$75,000 each to develop the regional Rappahannock Criminal Justice Information Network, which will expand regional wireless capabilities to law enforcement, fire and emergency medical services. Also, Rockingham County and the City of Harrisonburg will jointly receive \$100,000 to support a portion of a multi-million dollar project to build a regional 800 MHz communication system. And the City of Winchester and Frederick County will jointly receive \$60,500 for Phase 1 of the Shenandoah Valley Regional E-Safety Network, which will use an open architecture design to provide data interoperability.

Source: <http://www.govtech.net/news/news.php?id=93158>

### **27. *February 18, Elko Daily Free Press (NV)* — Radio problem threat to emergency services.**

According to the findings of a study funded by the Department of Energy and presented to Nevada's Elko County Board of Commissioners on Wednesday, February 16, there are serious flaws in Elko County's emergency communications system. The board was told there were numerous problems ranging from several of the mountain top repeaters not being legally

licensed to aged equipment to improperly installed equipment. Elko County also does not have a backup system in the event the primary system goes down. Another problem surfaced during consideration of getting the unlicensed sites licensed by the Federal Communications Commission (FCC). Licensing at some sites could prove difficult to accomplish because the FCC is no longer issuing licenses for outdated equipment in use at the unlicensed sites.

Source: [http://www.elkodaily.com/articles/2005/02/18/news/local/news\\_5.txt](http://www.elkodaily.com/articles/2005/02/18/news/local/news_5.txt)

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

## **Information Technology and Telecommunications Sector**

28. *February 24, K-Otik Security* — **Trend Micro products VSAPI ARJ archives processing vulnerability.** A critical vulnerability was reported in several Trend Micro products, and could be exploited by attackers or worms to execute arbitrary commands. The problem is due to a buffer overflow error in the ARJ archive file format parser when handling a specially crafted file name field in the local header, which could be exploited by attackers to execute arbitrary commands by sending a specially crafted ARJ archive to a vulnerable scanner. Upgrade to VSAPI 7.510: <http://www.trendmicro.com/download/engine.asp>  
Source: <http://www.k-otik.com/english/advisories/2005/0203>
  
29. *February 24, Cisco* — **ACNS denial of service and default admin password vulnerabilities.** Devices running Cisco Application and Content Networking System (ACNS) software may be vulnerable to Denial of Service (DoS) attacks and may contain a default password for the administrative account. Devices running ACNS software may be vulnerable to the DoS attacks while configured as a transparent proxy server, forward proxy server, or reverse proxy server. The administrative account default password does not require a software upgrade and can be changed by a configuration command for all affected customers. Vendor solutions available through link below.  
Source: [http://www.cisco.com/warp/public/707/cisco-sa-20050224-acnsd\\_os.shtml](http://www.cisco.com/warp/public/707/cisco-sa-20050224-acnsd_os.shtml)
  
30. *February 24, Associated Press* — **Nokia: China poised to be biggest market for mobile phones.** Mobile phone giant Nokia Corp. expects China will likely overtake the United States as its biggest market within three years, Chief Executive Jorma Ollila says. The Chinese market is already Nokia's second biggest market after the United States, and with the expected rollout of third-generation, or 3G networks, and the surge in new users, Nokia should keep its market share there strong, Ollila said. "During the next three years, I would not be surprised to see China become Nokia's largest market in net sales terms," he said, adding that mobile phone use there was expected to account for nearly one quarter of the estimated three billion subscribers worldwide it has forecast by 2010.  
Source: <http://www.washingtonpost.com/wp-dyn/articles/A49810-2005Feb24.html?nav=headlines>
  
31. *February 24, CNET News* — **Mozilla Firefox vulnerabilities patched.** The Mozilla Foundation released on Thursday, February 24, an update to the Firefox Web browser to fix several vulnerabilities, including one that would allow domain spoofing. The open-source project released Firefox 1.0.1 to fix, among other bugs, a vulnerability in the Internationalized

Domain Names (IDN), a standard for handling special character sets in domain names that lets companies register domain names that appear to be the same in different languages. The IDN vulnerability allowed an attacker to create a fake Website on a non-Microsoft browser in order to pull off a phishing scam. The update is available for Windows, Mac OS X and Linux at <http://www.mozilla.org>.

Source: [http://news.com.com/Firefox+fix+plugs+security+holes/2100-10.02\\_3-5589693.html](http://news.com.com/Firefox+fix+plugs+security+holes/2100-10.02_3-5589693.html)

## 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:** Microsoft released an out of cycle patch on Tuesday of this week for Windows XP Service Pack 2 and Windows Server 2003 systems to address an issue that can cause a computer to stop responding if certain firewall or anti-virus programs are installed on the machine. The following knowledgebase article discusses the patch: <http://support.microsoft.com/kb/887742>

To obtain the patch, please visit the following link:

<http://windowsupdate.microsoft.com>

The FBI is also reporting that emails claiming to be from its 'Internet Fraud Complaint Center' are actually virus-laden scams. The FBI never sends out unsolicited emails and asks that if you receive one of these bogus emails, please report it to the Internet Crime Complaint Center at <http://www.ic3.gov>.

### Current Port Attacks

<b>Top 10 Target Ports</b>	445 (microsoft-ds), 27015 (halflife), 20525 (----), 135 (epmap), 1025 (----), 139 (netbios-ssn), 53 (domain), 4672 (eMule), 80 (www), 37015 (----) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://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

32. *February 25, Wired* — **Web searchers find terror sites.** On the Website of Internet Haganah the mark of victory is a makeshift graphic — a little blue AK-47 assault rifle, which means another jihad Website taken out by going on the offensive. Aaron Weisburd runs Internet Haganah out of his southern Illinois home and describes Internet Haganah as a "small band of researchers, analysts, translators and consultants" around the globe dedicated to ferreting out Websites linked to terrorist groups. Since its inception three years ago, Internet Haganah has taken credit for or assisted in the shutdown of more than 600 sites it claims were linked to terror. Surprisingly, much of Internet Haganah's work is focused on the United States, where the cost of buying and maintaining a domain is cheap, and customers' privacy is guarded. "There are close to 300 sites listed in our database, and hundreds more that we are aware of and in the process of listing," Weisburd said. "Most of them are kept online by American companies." Experts say the presence of Islamic radicalism on the Web has grown markedly since 9/11. They say the Internet has become a vital means of communication, financing, and indoctrination for Islamic jihad, widely believed to be a decentralized movement.  
Source: <http://www.wired.com/news/privacy/0,1848,66708,00.html>

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

### **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 <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS/IAIP Daily Report Team at (703) 883-3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> 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](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.