



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 24 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

- The Wall Street Journal reports hospital patients are vulnerable to identity theft when their Social Security numbers are used as a medical identifier. (See item [4](#))
- The Associated Press reports Alabama will train 25 more troopers to recognize and detain illegal immigrants during traffic stops, a program that the Department of Homeland Security is hoping can be copied nationally. (See item [8](#))
- The San Diego Union Tribune reports a U.S. mail carrier was arrested on suspicion of identity theft, receiving stolen property, and drug possession for allegedly trading mail for drugs and other products. (See item [13](#))

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 23, Department of Energy* — **Government entity releases new monthly product.**
The Energy Information Administration (EIA) released a new product on Wednesday, February 23, called the Monthly Flash Estimates of Electric Power Data, which includes the most recent EIA electricity data. This product will be released approximately 45 days after the end of the reporting month, and serves as an early release (approximately 30 days) before the more detailed Electric Power Monthly report. The new release will present national-level data and

charts for the current month, as well as the previous month, year-to-date summation, and rolling 12-month information for electricity generation; fuel consumption; fuel stocks; electricity sales and revenue; average retail electricity prices; and a brief summary of the national-level data to put the information into a useful context. Monthly Flash Estimates of Electric Power Data is available at <http://www.eia.doe.gov/cneaf/electricity/epm/flash/flash.html>

Source: <http://www.eia.doe.gov/neic/press/press252.html>

- 2. February 23, Silicon Valley/San Jose Business Journal (CA) — Missing nuclear fuel rods may have been found.** After looking for seven months, Pacific Gas & Electric Co. says it may have found what remains of three missing nuclear fuel rods from its Humboldt Bay nuclear power plant near Eureka in Northern California. The three rods, which were 18 inches in length when they were taken out of service, apparently have been sitting at the bottom of the plant's used fuel pool since the 1960s. However, because they've been damaged by other used rods piled on top of them over the years, the utility isn't claiming they've really been found. "Based on an independent expert analysis of the fuel fragments we have recovered from the used fuel pool, it is most likely that we have the cut fuel rod segments in our possession. Unfortunately, their condition after 40 years of being stored under other components in the pool makes positive identification extremely difficult," said Greg Rueger, senior vice president for generation and chief nuclear officer. In a report to the Nuclear Regulatory Commission made public Wednesday, February 23, the utility also says security systems and procedures in place at the power plant were sufficient to detect and prevent attempted theft of the rods by either an internal or external party.

Source: http://www.bizjournals.com/sanjose/stories/2005/02/21/daily3_1.html

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

Chemical Industry and Hazardous Materials Sector

Nothing to report.

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

Defense Industrial Base Sector

Nothing to report.

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

Banking and Finance Sector

- 3. February 23, Asia Pulse — Australia still viewed as a soft target for money laundering.** While the risks are lower, Australia is still viewed as a soft target for money laundering and terrorism finance, conference attendees heard on Wednesday, February 23. Macquarie Bank senior economist Brian Redican said Australia was in a better position to handle a money laundering problem than in other jurisdictions, but said there was no room for complacency. Speaking at an Asia Pacific Private Banking conference held in Sydney, Redican told delegates that roughly two to five per cent of global Gross Domestic Product consisted of money

laundering — representing between about \$US11.11 billion to \$US31.74 billion annually. The rationale for money laundering includes organized crime, profits from drug trafficking, as well as terrorism, Redican said. While Australia's geographic isolation provided natural barriers to such criminal activity, financial institutions could not discount Australia being a target. "Australia is at the lower end of the spectrum, (but it) could also be seen as a soft target for Asian criminal elements," Redican said. ANZ general manager of group compliance Sean Hughes said the Financial Action Task Force on Money Laundering had already signaled that it believed Australia had to lift its game.

Source: <http://au.news.yahoo.com/050223/3/t771.html>

4. *February 23, The Wall Street Journal* — **Identity thieves find ways to target patients.**

Hospital patients are vulnerable to identity theft in part because they are unlikely to detect anything amiss. Some, such as terminally ill patients, may never leave the hospital. The biggest vulnerability of hospital patients is that their Social Security numbers often double as a medical identifier. For identity thieves, "Social Security numbers are the key to the golden kingdom," says Mari Frank, a California attorney specializing in identity theft. Of course, new technologies such as bar-coded wristbands and electronic medical records accessible only by password will help thwart identity theft. And the recently enacted Health Insurance Portability and Accountability Act, or HIPAA, pressures hospitals to improve patient privacy, and is expected to bring improvement. But social security numbers often continue to be used as patient identifiers. Often, the culprit in medical settings is a rogue employee. Identity-theft experts recommend that patients and loved ones protest any visible use of Social Security numbers, such as on wristbands or unguarded charts. Patients should refuse to answer aloud any verbal request for those numbers when they might be overheard. Patients should also resist the impulse to trust their fellow patients.

Source: <http://www.post-gazette.com/pg/05054/461706.stm>

5. *February 23, eWeek* — **Microsoft confirms browser phishing flaw.** Software engineers from Microsoft Corp.'s security research team have confirmed the existence of a bug in the Internet Explorer browser that opens the door to URL spoofing attacks. The flaw can be exploited by a malicious attacker to spoof the URL of a pop-up advertisement and has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP Service Pack 2. According to a Microsoft spokesperson, Windows XP SP2 requires the URL of pop-up ads to display in the title bar when a pop-up has been opened without the address bar. "Our early analysis indicates that only pop-up ads that contain extremely long URLs can be spoofed in this scenario," said a Microsoft spokesperson. There is no patch available yet to correct this issue.

Source: <http://www.eweek.com/article2/0.1759.1768963.00.asp>

6. *February 22, Associated Press* — **Illinois governor wants identity theft laws strengthened.**

Illinois Governor Rod Blagojevich said Wednesday, February 23, he wants state identity theft laws tightened after revelations that more than 5,000 Illinois residents could have had their personal information stolen as a result of a security breach at ChoicePoint. Blagojevich wants the state to require companies to notify people when their personal information is stolen from computer databases. Cases in which social security numbers, medical records or other personal information is being released through computer security failures or fraud are growing, he said. Blagojevich wants both in-state and out-of-state businesses to have to tell consumers if their

personal information gets compromised. There is no notification requirement now in Illinois.
Source: <http://www.chicagotribune.com/news/local/chi-050222idtheft.1.4225272.story?coll=chi-news-hed>

7. *February 21, The Wall Street Journal* — **Identity theft puts pressure on data sellers.**

Companies that compile and sell billions of private records on Americans could face new regulatory pressure in the wake of revelations by ChoicePoint Inc., one of the largest such information brokers, that an identity-theft ring gained access to tens of thousands of its electronic documents. The incident raises new alarms about companies that sell private data and their growing role as providers of information to law enforcement. Some critics believe the private data brokers have had too little government oversight and that all their databases should fall under regulations that govern credit reports. Senator Bill Nelson (D-FL) ordered his staff to study possible legislation that would expand the Federal Trade Commission's (FTC) regulatory power to oversee information brokers the way it does companies that handle financial and medical records. Marc Rotenberg, executive director of the Electronic Privacy Information Center in Washington, DC, a non-profit privacy watchdog group, wrote to the FTC in December seeking an investigation of ChoicePoint and other companies for compliance with the Fair Credit Reporting Act, which requires credit-report providers to vouch for the accuracy of their information. Now, he says, "this ends the discussion on whether self-regulation works."
Source: <http://www.post-gazette.com/pg/05052/460233.stm>

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

Transportation Sector

8. *February 23, Associated Press* — **Alabama to train more troopers for new immigration**

role. The state of Alabama will train 25 more troopers to recognize and detain illegal immigrants during traffic stops, a program that a Department of Homeland Security official is hoping can be copied nationally. Alabama volunteered for the program in September 2003 and has 21 immigration-trained troopers. Florida is the only other state to use troopers in immigration enforcement. "This has been a very successful experience and we hope this will become a model for the nation," said Homeland Security Undersecretary Asa Hutchinson. "Homeland Security should be about expanding our partnerships with the states." Alabama is estimated to have as many as 75,000 or 100,000 undocumented immigrants in the state, many of them working in agriculture and construction.

Source: <http://www.accessnorthga.com/news/hall/newfullstory.asp?ID=8.9578>

9. *February 23, Department of Transportation* — **Canadian St. Lawrence Seaway to open in**

March. The U.S.-Canadian St. Lawrence Seaway officially opens to commercial ships on March 25th. The world's longest waterway annually accounts for billions of dollars in revenue and supports tens of thousands of jobs in the eight Great Lakes states and two Canadian provinces of Ontario and Quebec. "We'll be ready for the safe and reliable movement of international and domestic marine traffic on opening day," said Albert Jacquez, Administrator of the Saint Lawrence Seaway Development Corporation, the Department of Transportation organization that owns and operates the two U.S. locks in Massena, NY. The Seaway's top priority is ensuring the safety and security of one of North America's premier inland waterways, the surrounding communities and the families living along its shores, he added. To

stay prepared, Jacquez said the Corporation provides emergency response training to its employees and regularly reviews and revises its Emergency Response Plan.

Source: <http://www.dot.gov/affairs/dot3005.htm>

10. *February 23, Government Accountability Office* — **GAO-05-324: Aviation Security: Measures for Testing the Impact of Using Commercial Data for the Secure Flight Program (Report)**. The Transportation Security Administration (TSA) is developing a new passenger prescreening program, known as Secure Flight. Under the Secure Flight program, TSA plans to take over, from commercial airlines, the responsibility for comparing identifying information of domestic airline passengers against information on known or suspected terrorists. To determine if the measures developed by TSA for commercial data testing are designed to identify impacts on aviation security, the Government Accountability Office (GAO) reviewed and analyzed TSA's draft statement of work for commercial data concept testing, which includes the initial measures developed by TSA. Since the purpose of the review was to determine whether the measures identify impacts on aviation security, GAO assessed the measures against performance measurement criteria previously developed by GAO based on best practices. On the basis of GAO's knowledge of the Secure Flight program and GAO performance measurement criteria, GAO determined whether TSA's measures are designed to reflect relevant impacts on aviation security and are consistent with attributes of successful performance measures. GAO conducted its work in accordance with generally accepted government auditing standards from December 2004 to February 2005. GAO is also continuing to review TSA's measures for commercial data testing based on a follow-on congressional request.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-05-324>

11. *February 23, Government Accountability Office* — **GAO-05-202: Homeland Security: Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant Status Indicator Technology Program (Report)**. The Department of Homeland Security (DHS) has established a program — the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) — to collect, maintain, and share information, including biometric identifiers, on selected foreign nationals who travel to the United States. By congressional mandate, DHS is to develop and submit for approval an expenditure plan for US-VISIT that satisfies certain conditions, including being reviewed by the Government Accountability Office (GAO). Among other things, GAO was asked to determine whether the plan satisfied these conditions and to provide observations on the plan and DHS's program management. To better ensure that the US-VISIT program is worthy of investment and is managed effectively, GAO is reiterating its previous recommendations and is making several new recommendations, including that DHS fully disclose in future expenditure plans its progress against previous commitments and that it reassess plans for deploying an exit capability. DHS concurred with GAO's findings and recommendations. Highlights: <http://www.gao.gov/highlights/d05202high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-05-202>

12. *February 22, USA TODAY* — **Despite new technology, border patrol swamped**. More than three years after the terrorist attacks in 2001, the 11,000 men and women who serve as the border's front-line defense are almost overwhelmed. Despite an influx of new technology, such as underground sensors and cameras that pan the desert, agents catch only about one-third of the estimated three million people who cross the border illegally every year. Most of the illegals

are poor Mexican laborers looking for work. But officials are alarmed that a growing number hail from Central and South America, Asia, even Mideastern countries such as Syria and Iran. In 2003, the Border Patrol arrested 39,215 so-called "OTMs," or other-than-Mexicans, along the Southwest border. In 2004, the number jumped to 65,814. Those figures worry intelligence and Department of Homeland Security officials, who say al Qaeda leaders want to smuggle operatives and weapons of mass destruction across the nation's porous land borders. And even as the Border Patrol has gotten new high-tech equipment, so have the people they're trying to catch. Smugglers use two-way radios, cell phones, global positioning systems and other high-tech equipment to watch agents' movements and alert each other when the coast is clear. Source: http://www.usatoday.com/news/nation/2005-02-22-border-patrol_x.htm

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

Postal and Shipping Sector

13. February 22, *San Diego Union Tribune (CA)* — Mail carrier held on suspicion of identity theft. A U.S. mail carrier was arrested on suspicion of identity theft, receiving stolen property and drug possession for allegedly trading mail for drugs and other products, it was announced Tuesday, February 22. Kenneth Herman who delivered mail in Pacific Beach and Point Loma, CA, was taken into custody Saturday, February 19, said District Attorney Bonnie Dumanis. The investigation into Herman's alleged activities was triggered when San Diego police Officer Chris Leahy noticed something amiss during an arrest in another case last month. He notified the district attorney's Computer and Technology Crime High-Tech Response Team, Dumanis said. Mail intended for residents on Herman's route in the beach area was found in his possession when he was taken into custody, authorities said. "That mail was then turned over to identity thieves who victimized residents on the mail carrier's route," Dumanis said. A broader investigation into Herman's activities has resulted in the recovery of significant quantities of methamphetamine; cash; a stolen passport; counterfeit financial documents; identification and checks; stolen mail; guns and ammunition; and the arrests of several others, according to a statement from the district attorney's office.

Source: http://www.signonsandiego.com/news/metro/20050222-1550-maila_rrest.html

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

Agriculture Sector

14. February 23, *Agricultural Research Service* — Medicinal compound used as fungicide. Growers of many fruit and ornamental crops have new weapons for fighting destructive fungi, thanks to Agricultural Research Service (ARS) and University of Mississippi (UM) scientists who've transformed a medicinal compound into an agricultural fungicide. The naturally occurring compound, called sampangine, was first patented by UM in 1990 as a treatment for human fungal infections. It was never released pharmaceutically. Now, plant pathologist David Wedge of ARS and UM associate professor Dale Nagle have been issued a patent for sampangine and similar, related compounds as broad-spectrum, low-toxicity controls of fungal plant pathogens that threaten agriculture. According to the new patent, sampangine-based compounds can control such fungi as *Botrytis cinerea*, which causes gray mold on tomatoes;

Colletotrichum fragariae, which produces anthracnose crown rot and wilt in strawberry plants; *C. gloeosporioides*, which sickens numerous plants, including grapes, strawberry, citrus, and papaya; and *Fusarium oxysporum*, which induces vascular wilt in crops such as potato, sugarcane, and many ornamentals. Sampangine can greatly help the United States' \$31-billion-a-year minor crop industry.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

15. *February 22, Ohio State University* — **Corn diseases making a comeback.** Corn diseases are finding their way back into Ohio fields, mainly because some current hybrids lack resistance. “High yielding hybrids are such a focus now that selecting for effective resistance to these diseases has been de-emphasized in the breeding process, and now they are showing up uncontrolled in certain fields.” said Peter Thomison, an Ohio State agronomist. Northern corn leaf blight can cause upwards of 40–50 bushel-per-acre yield losses in the most severe cases. Northern corn leaf blight was brought under control with the development of both partial resistance and a race specific resistance gene, called Ht. By the early 1980s, however, the fungus had developed a new race, called Race 1, which was causing susceptible lesions on hybrids with the Ht gene. Inoculation tests were conducted on hybrids. “We found that two-thirds of 71 hybrids evaluated showed the susceptible lesion type,” said Pat Lipps, a plant pathologist. “What that is telling us is that a majority of the hybrids being used by growers in the state are likely susceptible to the prevalent race of northern leaf blight.” Diplodia ear rot is has also become more aggressive in recent years. Diplodia ear rot affects the grain quality and yield.

Source: <http://www.ag.ohio-state.edu/~news/story.php?id=3041>

16. *February 18, Journal of Clinical Microbiology* — **Test may differentiate between poultry vaccinated against or infected with avian flu.** Vaccination programs for the control of avian influenza (AI) in poultry have limitations due to the problem of differentiating between vaccinated and virus-infected birds. Researchers used NS1, the conserved nonstructural protein of influenza A virus, as a differential diagnostic marker for influenza virus infection. Experimentally infected poultry were evaluated for the ability to induce antibodies reactive to NS1 recombinant protein produced in *Escherichia coli* or to chemically synthesized NS1 peptides. Immune sera were obtained from chickens and turkeys inoculated with live AI virus, inactivated purified vaccines, or inactivated commercial vaccines. Seroconversion to positivity for antibodies to the NS1 protein was achieved in birds experimentally infected with multiple subtypes of influenza A virus, as determined by enzyme-linked immunosorbent assay (ELISA) and Western blot analysis. In contrast, animals inoculated with inactivated gradient-purified vaccines had no seroconversion to positivity for antibodies to the NS1 protein, and animals vaccinated with commercial vaccines had low, but detectable, levels of NS1 antibodies. The use of a second ELISA with diluted sera identified a diagnostic test that results in seropositivity for antibodies to the NS1 protein only in infected birds. These results demonstrate the potential benefit of a specific ELISA for anti-NS1 antibodies that may have diagnostic value for the poultry industries.

Source: <http://jcm.asm.org/cgi/content/abstract/43/2/676>

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

Food Sector

17. *February 23, Business Wire* — **Small business task force on food safety created.** Mark Taggatz, CEO of e-FoodSafety.com, Inc., a Palm Springs, CA, based company announced Wednesday, February 23, that he has created a Small Business Task Force on Food Safety. Taggatz will serve as Chairman of the Task Force with its headquarters in Palm Springs and a Government and Public Affairs office in Washington, DC. "We are enlisting a wide range of small company leaders who are involved in food safety within the technology, manufacturing, distribution, retailing, service, and consulting sectors to join our Task Force," Taggatz says. Taggatz also explains the Task Force's mission is to address pertinent food security issues, provide participants with useful information about the impact of the Bioterrorism Act on the food industry, and enhance communications among the food industry, regulators, and academia. Source: http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20050223005217&newsLang=en

18. *February 18, Applied and Environmental Microbiology* — **Prevalence of Salmonella in oysters in the U.S.** Food-borne diseases such as salmonellosis can be attributed, in part, to the consumption of raw oysters. To determine the prevalence of Salmonella spp. in oysters, oysters harvested from 36 U.S. bays (12 each from the West, East, and Gulf coasts in the summer of 2002, and 12 bays, four per coast, in the winter of 2002–2003) were tested. Salmonella was isolated from oysters from each coast of the U.S., and 7.4 percent of all oysters tested contained Salmonella. Isolation tended to be bay specific, with some bays having a high prevalence of Salmonella, while other bays had none. The vast majority (78/101) of Salmonella isolates from oysters were Salmonella enterica serovar Newport, a major human pathogen, confirming the human health hazard of raw oyster consumption. Source: http://aem.asm.org/cgi/content/abstract/71/2/893?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=&fulltext=oyster&searchid=1109178833963_6303&stored_search=&FIRSTINDEX=0&volume=71&issue=2&journalcode=aem

[[Return to top](#)]

Water Sector

19. *February 22, Associated Press* — **Ohio authorities blame groundwater for Lake Erie island outbreak.** Drinking water contaminated by sewage and other pollution was the likely source of an outbreak that sickened 1,400 people on Lake Erie's South Bass Island the summer of 2004, Ohio Health Department officials said Tuesday, February 22. Tourists and residents were stricken with fever, diarrhea and vomiting after visiting the island, which is about halfway between Toledo and Cleveland. The island's wells, which supply water to about 400 vacation homes and businesses, were tainted when porous soil allowed sewage from septic systems and runoff containing bird droppings and lawn fertilizer to infiltrate groundwater, the department said. In tests of private wells, investigators found that eight of 10 contained bacteria, including E. coli in some cases. The main tourist area relies on the municipal water system. Officials are pushing a \$5.2 million project to expand the municipal system to all island businesses. It is expected to be finished in about two years. Source: http://news.yahoo.com/news?tmpl=story&u=/ap/20050223/ap_on_r_e_us/island_illnesses_1

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

Public Health Sector

20. *February 23, Associated Press* — **Coordination urged in fight against bird flu.** Speaking at the opening of a three-day bird flu conference in Ho Chi Minh City, Shigeru Omi, the World Health Organization's (WHO) Western Pacific regional director, said it is critical that the international community coordinate its fight against the virus. "We at WHO believe that the world is now in the gravest possible danger of a pandemic," Omi said. The bird flu has killed 45 people in Asia over the past year, in cases largely traced to contact with sick birds, and experts have warned the H5N1 virus could become far deadlier if it mutates into a form that can be easily transmitted among humans. "We are urging all governments to work now on a pandemic preparedness plan — so that even in an emergency they will be able to provide basic public services such as transport, sanitation, and power," he said. "There is an increasing risk of avian influenza spread that no poultry-keeping country can afford to ignore," said Samuel Jutzi, of the Food and Agriculture Organization (FAO). Jutzi said the avian flu virus will persist in Asia for years and coordinated efforts need to focus on controlling it at its source — in animals.
Source: http://www.washingtonpost.com/wp-dyn/articles/A46424-2005Feb_23.html

21. *February 22, PLoS Medicine* — **Mass spectrometry-based SARS genotyping.** To quickly control infectious disease outbreaks, extensive information is required to identify the source and transmission routes, and to evaluate the effect of containment policies. Traditionally, scientists have used travel- and contact-tracing methods, but the recent Severe Acute Respiratory Syndrome (SARS) epidemic showed that sequence-based techniques for pathogen detection can also be important tools to help understand outbreaks. Scientists adapted mass spectrometry (MS)-based genotyping, already used as a high-throughput way of detecting single nucleotide polymorphisms in human DNA, to the analysis of the SARS virus from clinical samples. The scientists analyzed isolates taken from 13 patients with SARS at different stages of the Singapore outbreak, identified nine sequence variations, and discovered a new primary route of introduction of the virus into the Singapore population. They also found a Singaporean origin for a German case of SARS, a result that could not be derived from standard sequencing methods. The study suggests that MS-based genotyping can be used for large-scale genetic characterization of viral DNA from clinical samples. The scientists found that the method was accurate and sensitive, with a 95 percent success rate for detecting sequence variations at low virus concentrations. It is particularly useful for investigating agents for which extensive sequence information exists.
Source: <http://medicine.plosjournals.org/perlserv/?request=get-document&doi=10.1371/journal.pmed.0020052>

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

Government Sector

22. *February 23, Department of Homeland Security* — **Appointments to Data Privacy and Integrity Advisory Committee.** The Department of Homeland Security (DHS) on Wednesday,

February 23, announced the appointment of twenty members to the Data Privacy and Integrity Advisory Committee (DHS Privacy Advisory Committee). This newest federal advisory committee to DHS was established to provide external expert advice to the Secretary and the Chief Privacy Officer on programmatic, policy, operational, and technological issues that affect privacy, data integrity, and data interoperability in DHS programs. The members of this Advisory Committee have diverse expertise in privacy, security, and emerging technology, and come from large and small companies, the academic community, and the non-profit sector. The members also reflect a depth of knowledge on issues of data protection, openness, technology, and national security.

Source: <http://www.dhs.gov/dhspublic/display?content=4367>

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

Emergency Services Sector

23. *February 23, Star Telegram (TX)* — Projects selected for possible security funding. Regional emergency preparedness officials on Tuesday, February 22, finalized a list of 145 projects in the Dallas/Fort Worth Metroplex area to share about \$30 million in Department of Homeland Security funding. The projects, funded through Texas state and federal Homeland Security grants, are meant to help local agencies prevent and respond to potential terrorist attacks. But the money also helps fund first responders' ability to react to a variety of disasters. The projects that were selected include creating a bomb squad in Arlington, setting up a bioterrorism lab in Dallas, and improving security at water-treatment facilities. The list of projects must next be approved by officials in Austin. The selection committees included officials from police, fire, utility and transportation departments, and emergency management coordinators, health officials and some private industry members. Strict guidelines require that the funds be used on projects that affect a region rather than a specific city or town, and recipients must have mutual aid agreements.

Source: <http://www.dfw.com/mld/dfw/news/10969927.htm?1c>

24. *February 23, Pittsburgh Post-Gazette (PA)* — Northwest Pennsylvania ready for merger. Ambulance drivers, firefighters, police officers and paramedics serving six communities should will hear familiar voices next month as Northwest Regional Communications is absorbed into Allegheny County's 911 system. The expanded system could start operation as soon as mid-March and be fully integrated by the end of the month. Northwest serves Coraopolis, Crescent, Findlay, Moon, Neville, Robinson in the West and 18 communities north of the Ohio River. All 16 full- and part-time dispatchers and two administrators who work for Northwest have applied to join the county team, according to Daniel Nussbaum, Northwest's communications director. First responders in member communities will be able to use existing equipment and will hear the same dispatcher voices, Nussbaum said. The merger of Northwest into the county system represents the latest chapter in regional consolidation of emergency dispatch services. Allegheny County, with its 133 municipalities, was among the last metropolitan areas in the country to inaugurate 911 emergency services. Before 1998, those seeking emergency assistance in the county had to dial as many as 10 digits to reach ambulance, police or firefighting services.

Source: <http://www.post-gazette.com/pg/05054/461280.stm>

25. *February 23, Mooresville/Decatur Times (IN)* — **Indiana state police receive new bomb unit.**

The Indiana State Police Explosive Ordnance Disposal Team is now better equipped to serve the state in finding, investigating, and disposing of hazardous devices. "With money from a Homeland Security grant, the department purchased the high-tech equipment required for team members to safely do their job," said Indiana State Police Trooper Richard Myers. The grant, totaling \$886,000, was used to purchase bomb search suits, response vehicles, portable x-ray units, specialized hand tools and a variety of other equipment to assist team members in the investigation of suspicious devices. The specially designed bomb suits protect team members from fragments and the force of the blast. The 10 response vehicles will be located across the state and will carry the necessary equipment to respond to a wide variety of hazardous device calls. State police bomb squad members are dispatched often every year to investigate bomb threats, dignitary protection services, recovery of military and commercial explosives and improvised explosive devices.

Source: http://www.md-times.com/?module=displaystory&story_id=7612&format=html

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

Information Technology and Telecommunications Sector

26. *February 23, K-Otik Security* — **vBulletin "misc.php" remote PHP code injection**

vulnerability. A new vulnerability was identified in vBulletin, and may be exploited by remote attackers to execute arbitrary PHP commands. The flaw resides in the "Add Template Name in HTML Comments" option when handling the "template" (misc.php) parameter, which may be exploited to execute arbitrary php commands with the web server privileges. Update to version 3.0.7: <http://www.vbulletin.com>

Source: <http://www.k-otik.com/english/advisories/2005/0192>

27. *February 23, K-Otik Security* — **phpBB2 arbitrary file unlink and disclosure**

vulnerabilities. Two vulnerabilities were identified in phpBB, and may be exploited by remote attackers to read or deleted arbitrary system files. The first flaw is due to an input validation error when handling specially crafted requests to upload avatars, which may be exploited by attackers to read arbitrary system files. The second vulnerability is due to a directory traversal error when handling the "avatarselect" return value, which may be exploited by attackers to unlink arbitrary system files. Updates to phpBB version 2.0.12:

<http://www.phpbb.com/downloads.php>

Source: <http://www.k-otik.com/english/advisories/2005/0194>

28. *February 22, Reuters* — **Singapore unveils plan to battle cyber terror.** Singapore is to spend \$23 million over three years to battle online hackers and other forms of "cyber-terrorism" in one of the world's most connected countries, government officials said Tuesday, February 22. Describing the infrastructure behind the Internet as a "nerve system" in Singapore, Deputy Prime Minister Tony Tan said a new National Cyber-Threat Monitoring Center would maintain round-the-clock detection and analysis of computer virus threats. Singapore has one of the world's highest Internet penetration rates, with 50-60 percent of its 4.2 million people living in homes wired to the Internet. The Cyber-Threat Monitoring Center will link up with companies that provide anti-virus systems and governments running similar centers, including the United States and Australia. It is expected to be fully operational by the second half of 2006.

Source: <http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=7698536>

29. *February 22, Secunia* — **cURL/libcURL NTLM and Kerberos authentication buffer overflows.** Two vulnerabilities have been reported in cURL/libcURL 7.12.1, which can be exploited by malicious people to compromise a user's system. Boundary errors in the "Curl_input_ntlm()" and the "Curl_krb_kauth()" function can be exploited to cause a stack-based buffer overflow. Updates available at:

http://cool.haxx.se/cvs.cgi/curl/lib/http_ntlm.c.diff?r1=1.36&r2=1.37

Source: <http://secunia.com/advisories/14364/>

30. *February 22, Associated Press* — **FBI officials warn about computer virus.** The FBI warned Tuesday, February 22, that a computer virus is being spread through unsolicited e-mails that purport to come from the FBI. The e-mails appear to come from an fbi.gov address. They tell recipients that they have accessed illegal Websites and that their Internet use has been monitored by the FBI's "Internet Fraud Complaint Center," the FBI said.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A45131-2005Feb22.html>

31. *February 22, Federal Computer Week* — **Federal government to hold cyber preparedness exercise.** The federal government and several international partners will hold a cyber preparedness exercise in November, Department of Homeland Security (DHS) officials said at the RSA Conference in San Francisco last week. Its purpose is to give federal agencies an opportunity to test their plans for responding to a direct or indirect attack on the computer networks that control the nation's critical infrastructure such as power plants and oil pipelines. The exercise will be unclassified, and the public will be informed, said Hun Kim, deputy director of the National Cyber Security Division at DHS. The RSA Conference brings together IT professionals from industry, academia, and government to share information and exchange ideas on technology trends and best practices in IT security.

Source: <http://www.fcw.com/fcw/articles/2005/0221/web-cyber-02-22-05.asp>

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>

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 139 (netbios-ssn), 22321 (wnn6_Tw), 1025 (----), 53 (domain), 80 (www), 4662 (eDonkey2000), 1026 (----), 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.