Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 27 February 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- USA Today reports a panel of vaccine experts will explore the possibility of recommending annual flu vaccinations for all Americans, which would improve overall vaccination rates and prepare the public health system for mass vaccinations if a flu pandemic should strike. (See item 23)
- Click2Houston reports a man was charged on Wednesday after he allegedly told a security guard near the Texas Medical Center in Houston that he had the makings for a dirty bomb. (See item 29)
- The Associated Press reports Interpol is setting up a new alert system of computer−delivered alerts to keep its 181 member nations up to date on rapidly changing techniques and technologies used around the world. (See item 33)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; 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 and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web 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, WXIA−TV (GA)* — **Power outages increase to over 20,000. Up to 24,000 Georgia Power customers were left without power Thursday, February 26, as snow, ice and gusting winds sweep through northern regions. A Georgia Power spokesperson said a bulk of the reported outages −− about 9,000 −− are south of Metro Atlanta. Within**

Atlanta, about 5,000 outages are reported, and to the north, Georgia Power estimates about 2,000 outages. "Basically, what we're battling now is the road conditions. It's kind of a treacherous situation for our crews and it's really slowed down progress for us to getting these areas to get these power lines off the roads," Georgia Power spokesperson Lynn Wallace said. Wallace said a combination of powerful winds and snow brought large trees and limbs down onto power lines. In some places, however, the severe winter weather proved harsh enough to snap the power line poles.
Source: http://www.11alive.com/news/news_article.aspx?storyid=43430

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

2. *February 26, Navy News Stand* — **Navy establishes cryptologic technician networks rating. In another force−shaping move, the Navy announced the establishment of the Cryptologic Technician Networks (CTN) rating in February. The new rating, which became effective February 6, is designed to further develop a skilled work force to meet fleet requirements in computer network defense and other computer network operations.** It also supports the Chief of Naval Operations' guidance to transform information operations. That mission area is currently being performed by the Cryptologic Technician (Communications), Cryptologic Technician (Maintenance) and Cryptologic Technician (Administration) ratings. As Sailors convert over time to CTN, these legacy ratings will be collapsed and disestablished. "Creation of the CTN rating is a positive move toward consolidation of CT skills," said Chief of Naval Personnel, Vice AdmiralGerry Hoewing. "Establishment of a single rating is the most effective and efficient way to engage the types of information technology and computer network threats we face in this new century."
Source: http://www.news.navy.mil/search/display.asp?story_id=12047

3. *February 26, Federal Computer Week* — **Military: JTRS not about the box. Air Force and Navy officials want a software radio that gives improved voice and data−sharing capabilities so they can better carry out the military's emerging network−centric warfare doctrine. The services do not want the Joint Tactical Radio System's (JTRS) airborne and maritime/fixed station (AMF) radio to simply let airmen and sailors use one device to speak and send data** on frequencies from 2 MHz to 2 GHZ, said Air Force Lt. Colonel Maryann Watson, AMF JTRS program manager. "We're not doing this for radios," Watson said. "We're doing this for capability. We don't want a new box." The Air Force, Navy and Army must buy 13,000 new radios for 75 aircraft, 50 ships and 20 fixed stations. Officials want industry to design the AMF radios with similar form, fit and functions, Watson said. However, they do not want to constrain companies during the 65−month program. They want vendors to keep the same framework for the radios, but they can provide different casings and accessories, she said. **Department of Defense officials want to build radios defined more by software**

than hardware so they can be more easily updated for new frequencies or functions.
Source: http://www.fcw.com/fcw/articles/2004/0223/web−jtrs−02−26−04. asp

4. *February 25, Federal Computer Week* — **Military certifies biometric profile. Officials at the Department of Defense's (DoD) Biometrics Management Office announced that the National Information Assurance Partnership has certified the first of five planned biometric protection profiles for DoD and other government agencies.** The U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments specifies minimum security requirements for virtual environments. A protection profile establishes the information assurance criteria for a given "class" of product, ensuring agencies don't buy devices that create security risks.
Source: http://www.fcw.com/fcw/articles/2004/0223/web−biomet−02−25−0 4.asp

[Return to top]

Banking and Finance Sector

5. *February 27, New Haven Register (CT)* — **International online scam involving job seeker. Police in Milford, CT, are urging the public to use caution when making transactions over the Internet. Police issued the warning Wednesday, February 25, after a five−month investigation into allegations that a Milford resident, who was not identified, was posting items for sale at the Internet auction site eBay but failing to deliver the merchandise when money was sent.** Police searched the Milford resident's home and seized several computers. However, according to police, the evidence on the computers served to bolster the suspect's story, rather than incriminate her. The woman told police that she had posted an ad on the job Website monster.com, seeking employment, and was contacted via e−mail by a person purporting to be the owner of a company called Valco, located in Colorado. The e−mail address of the purported owner was "commerce−1@yahoo.com." **The Milford resident told police that Valco hired her to receive checks and money orders from its customers and cash them, sending the money to various names and addresses in Russia.** According to police, the Milford resident believed this was a bona fide business and made the transactions. According to police, Valco Company is a fictitious name and the eBay accounts were fraudulent.
Source: http://www.zwire.com/site/news.cfm?BRD=1281&dept_id=517514&newsid=11026875&PAG=461&rfi=9

6. *February 26, Seattle−Post−Intelligencer (WA)* — **E−mail scam spoofs billing service. A new spoof cropped up last week, claiming that the e−mail recipient had just purchased a $3,000 notebook computer. The e−mail claims that the purchase was not completed because the retailer is having problems with its delivery company and asks the so−called buyer to request a refund through another Website.** The second Website looks like a page for a legitimate company called Jettis, which offers secure and confidential online billing options. To obtain a refund, the site reads, e−mail recipients must provide their name and credit card information. A Jettis attorney says the company is working with federal authorities to track down the source of this fraud site. Company engineers believe the site originated in Eastern Europe.
Source: http://blog.seattlepi.nwsource.com/consumer/archives/001539. html

7. *February 25, The Register (UK)* — **Skimmers attached to ATMs at university. A report out of the University of Texas at Austin warns students to look out for some savvy ATM bandits. The thieves are attaching their own equipment −− "skimmers" −− to the front of ATM machines and then transmitting data wirelessly to a nearby car.** The faux card reader sends back card number information, while a wireless camera mounted in a fake pamphlet holder sends back PIN information. "The thieves copy the cards and use the PIN numbers to withdraw thousands from many accounts in a very short time directly from the bank ATM," the school warns. Report: http://www.utexas.edu/admin/utpd/atm.html
Source: http://www.theregister.co.uk/content/28/35850.html

8. *February 23, Star−Telegram (TX)* — **Police seek help in solving rash of ATM robberies. Automated teller machines (ATMs) have become targets in recent months for smash−and−grab bandits, and police are asking the public for help in finding them. The thieves often steal a pickup or sport utility vehicle, crash it into a store and hit the ATM, throw the wrecked ATM into the vehicle and flee.** The Tarrant (TX) Regional Auto Theft Task Force announced a new push Friday, February 20, to track the criminals. "This has become far too commonplace in Tarrant and surrounding counties," said Jerry McCurry, the task force commander. **McCurry said at least 20 such incidents have occurred in the area since May, most since November. At least half the incidents have been in Fort Worth,** said Lt. Abdul Pridgen, Fort Worth police spokesperson. McCurry said store owners are being advised to install crash−resistant posts outside, to anchor ATMs to the floor more securely, to install more video cameras and alarms, and to remove money from the ATMs after closing hours.
Source: http://www.dfw.com/mld/startelegram/news/local/8019371.htm

[Return to top]

Transportation Sector

9. *February 26, The Journal (Newcastle−upon−Tyne, UK)* — **Trolley out of control on Metro.** Union leaders last night stepped up calls for a public inquiry into runaway trains after an unmanned trolley carrying tons of scrap went out of control on the Tyne and Wear Metro line. **The Rail Maritime and Transport (RMT) union said the latest incident in which a vehicle which ran for over a mile between Gateshead and Newcastle, through the city's Central Station, showed the urgent need for a public investigation.** Union officials said they were shocked to hear of the incident, which happened before Christmas but was only revealed yesterday. The RMT has been calling for a public inquiry since an accident earlier this month when four workers were killed by a runaway vehicle in Tebay, Cumbria. Bob Crow, general secretary of the RMT, said: "It beggars belief that so many incidents are now coming to light after apparently being hushed up at the time. It is now imperative that a public inquiry is held." The runaway trolley was of a type known to railwaymen as 'silent death' because it cannot be heard. It did not have brakes and has now been scrapped. Union officials compared the scare to the horrific accident on the West Coast Main Line in Cumbria 10 days ago when four railway workers were killed.
Source: http://cnniw.yellowbrix.com/pages/cnniw/Story.nsp?story_id=47583172&ID=cnniw&scategory=Transportation:Rail&

10. *February 26, Oakland Tribune* — **Ferries would reap biggest piece of toll.** California's Regional Measure 2, the proposed $1 bridge toll increase on the March ballot, would shower $680 million during the next 30 years on a public transit system few people use −− ferry boats crossing the Bay. Multimillion−dollar beneficiaries of the public funds generated by Measure 2 would include ferries that launch from Oakland and Alameda and a new service planned for Berkeley. BART is to receive just $392 million from Measure 2 −− all for capital improvement projects, while ferries could haul in at least $468 million in the next three decades for daily operations costs alone. **Ferry advocates say an expansion of the Bay ferry system will make it more convenient, attract more riders and make the ferries more cost−efficient. "People will ride ferries who won't necessarily ride BART or buses,"** said Steve Castleberry, executive director of the San Francisco Bay Area Water Transit Authority, one of the primary backers of Measure 2.
Source: http://cnniw.yellowbrix.com/pages/cnniw/Story.nsp?story_id=47598914&ID=cnniw&scategory=Transportation:Mass+Transit&

11. *February 26, Charlotte Business Journal (Charlotte, NC)* — **Charlotte crash blamed on maintenance lapse. A fatal airplane crash at Charlotte's airport in January 2003, was caused by incorrect maintenance, according to findings released Thursday by the National Transportation Safety Board (NTSB).** All 21 people on board the plane died. The plane, en route from Charlotte, NC, to Greenville−Spartanburg, SC, crashed shortly after takeoff at Charlotte Douglas International Airport. The NTSB's report says the probable cause of the crash was the airplane's loss of pitch control during takeoff, caused by incorrect rigging of the elevator control system. Mesa Air Group's Air Midwest carrier operated the flight as US Airways Express flight 5481. The NTSB says Air Midwest's and the Federal Aviation Administration's lack of oversight of the work being performed at Air Midwest's maintenance facility in Huntington, WA, contributed to the crash. It says the airplane's elevator control system had been incorrectly rigged during earlier maintenance there.
Source: http://charlotte.bizjournals.com/charlotte/stories/2004/02/2 3/daily50.html

12. *February 26, Reuters* — **European airports push for government security funding. European airports need the kind of government funding U.S. airports are receiving to keep pace in raising security for air travellers, airports association ACI Europe said on Thursday, February 27.** "Government assistance with the funding of anti−terrorist security measures is essential for Europe's airports. U.S. airports are clearly enjoying a significant competitive advantage," John Hume, director of policy at ACI Europe, said in a statement. Changing security needs are pushing airports to introduce sophisticated new equipment, such as a system being tested at Sweden's Umea Airport that identifies boarding passengers by matching their iris with an image of it printed on a smart card carried by the passenger. "The European airport industry has been faced with hundreds of millions of euro in costs for additional security measures and it is expected that such costs will continue to grow," the ACI said. "In contrast to the USA, most European governments have so far refused to bear the costs for these measures." **The costs being forced on airports reflect broad security needs that governments need to fund, Hume said. "These costs must not be passed directly on to airports and air passengers."**
Source: http://news.airwise.com/stories/2004/02/1077790839.html

13. *February 26, KVIA TV (El Paso, TX)* — **Train derails, more than two dozen freight cars scattered.** A Union Pacific Train derailed in the Lower Valley, and it has left a monstrous mess to clean up. The derailment happened a short while after 5 a.m. Thursday, February 26, between Ivey and Inglewood, under the Americas overpass. Railroad officials said it could take several days before the area is completely cleared. A total of 28 cars went off the tracks. Officials say the cars were carrying consumer products, but an initial concern was that they were packed with hazardous materials. Ultimately none the cars posed a serious threat, police said. **"They did have five vehicles that contained hazardous materials but those vehicles are on the tracks," said Javier Sambrano, a spokesman for the El Paso Police Department. "Those cars were not affected, so everything checked out okay with those vehicles."** The derailed cars also knocked some power lines down −− leaving area residents and businesses without power for several hours. Police say two people were inside the train when it derailed. Neither of them were injured.
Source: http://www.kvia.com/Global/story.asp?S=1671681&nav=AbC0L7NX

14. *February 26, Associated Press* — **Airline explores tolerance for frill−free flying.** Ryanair, Europe's most successful budget airline, is testing the Spartan spirit of its passengers and extending the frontiers of cost−cutting. **It recently announced it will dispense with the plane's window blinds, reclining seats, Velcro−anchored headrest covers, and the seat pockets where customers normally find a safety notice and free magazines. The required safety notice will be stitched to the back of each seat.** Removing such "nonessential extras" from its new Boeing 737s will save Ryanair hundreds of thousands of dollars per plane in the purchase price and the maintenance normally required on broken reclining seats, said Paul Fitzsimmons, the airline's chief spokesman. **Many of the cabin features are set by regulations covering seat belts, environmental−control systems, lighting and the number of doors. Beyond that, an airline is free to decide what amenities, if any, passengers will get on board, including toilets, closets and in−flight entertainment.** Ryanair offers its customers no assigned seats, no free food or drinks, no frequent−flyer miles and no help with connecting flights. It flies to secondary airports, has strict baggage weight limits, issues most tickets over the Internet and doesn't use enclosed ramps to take its customers from terminals to airplanes.
Source: http://www.cnn.com/2004/TRAVEL/02/26/bi.no.frills.airlines.a p/index.html

[Return to top]

Postal and Shipping Sector

15. *February 26, Associated Press* — **Postal Service seeks anti−terrorism funds.** Postmaster General John Potter appealed to Congress on Thursday, February 26, to provide anti−terrorism funds. **Potter asked for $779 million to help the agency buy and install systems to detect biological agents and poisons, and new ventilation and filtration systems, in 282 mail handling centers across the country.** Potter said his agency has developed the new detection and filtration systems and test installations are under way in Baltimore, MD, and Cleveland, OH. The current systems are designed to test for anthrax, he said, but improvements are being made to test for a variety of other likely materials. The post office has already signed contracts for more than $300 million of the requested money, Potter said, and if it is not provided, the agency will have to add the spending in when planning postal rate increases in the future.

Source: http://www.mlive.com/newsflash/lateststories/index.ssf?/base/politics−1/1077823142152930.xml

16. *February 25, Associated Press* — **Ruling protects Postal Service. The U.S. Supreme Court ruled Wednesday, February 25 that the Postal Service, as a part of the federal government, cannot be taken to court for alleged anticompetitive practices.** The loser in the unanimous decision was a mail sack−making company that claimed it was cheated when the Postal Service canceled its contract and started getting cheaper sacks made in Mexico. Flamingo Industries contends the new sacks do not meet safety and quality regulations and that other companies were not allowed to bid for the work. Justice Anthony M. Kennedy used the case to trace the history of America's mail service, back to the appointment of Benjamin Franklin as the first postmaster general in 1775. He said that the Postal Service is an independent part of the government that does not try to make money. It may be sued under federal antitrust laws, he said, only if Congress specifically allows it.
Source: http://www.sunherald.com/mld/sunherald/news/politics/8039867 .htm

[Return to top]

Agriculture Sector

17. *February 26, Bristol University* — **Stress gene found in plants.** A single gene has been discovered that helps plants cope with stressful situations such as disease or poor environments. Scientists at the universities of Bristol and Oxford isolated and characterised the gene called OXI1 from thale cress, a common weed. OXI1 boosts the plant's ability to stop fungal infection from spreading, and helps roots to grow despite poor conditions. **Claire Grierson from Bristol University said: "This is a significant advance from traditional approaches, where investigators have to identify a different gene for each disease or stress they hope to fight. At Bristol we showed that the gene is not just important for overcoming disease, but is also involved in another type of stress, growing in difficult conditions."** Thale cress (Arabidopsis thaliana) was the first plant to have its entire genetic code read. This understanding has already enabled biologists to protect wheat from disease and to double the yield of oilseed rape. Studying the OXI1 gene will help them understand more about how plants and other organisms deal with stress.
Source: http://www.innovations−report.com/html/reports/life_sciences /report−26282.html

[Return to top]

Food Sector

18. *February 26, Food Navigator* — **Bar codes to battle foodborne diseases.** Traceability has become a key concern in the meat processing industry since the mad cow disease outbreak in the United Kingdom in the 1990s, and more recently the discovery of the disease in the U.S. in December. A number of diagnostic products have been developed to create viable tracing systems to control any potential outbreak in the future. **A UK technology company has developed bar−coded cards that can be used to collect blood samples from live cattle while moving through production.** During the slaughter process and case−ready production, cattle

DNA is collected by the company's FTA system and then pressed onto the bar−coded cards. These are then stored in a file cabinet for analysis and auditing. Once the product has been packaged for retail sale, the final DNA profile is examined and compared to earlier samples for quality control. **The company has also entered into a cooperative research and development agreement with the U.S. Food and Drug Administration to develop of a universal template preparation protocol for the detection of human pathogens, such as bacteria, found in foods and water. Whatman hopes that once complete, the method could be applied to most, if not all, food matrices.**
Source: http://www.foodnavigator.com/news/news−NG.asp?id=50201

19. *February 25, Reuters* — **USDA mulls another expansion of mad cow testing.** The U.S. Agriculture Department (USDA) is considering a one−year plan to boost cattle testing for mad cow disease beyond the 40,000 head it planned to sample this year, Agriculture Secretary Ann Veneman said on Wednesday February 25. **An international review panel has recommended that the USDA test all "at risk" cattle older than 30 months for one year to establish the prevalence of mad cow disease in the United States. Veneman told a House Appropriations subcommittee that she may craft "a one−year testing program that would give us that baseline that was recommended in the report."** Veneman said funding for a one−year testing program would come from the USDA's Commodity Credit Corporation. After the program ends, annual testing would return to 40,000.
Source: http://www.agriculture.com/worldwide/IDS/2004−02−25T200241Z_01_N25341680_RTRIDST_0_MADCOW−USA−TESTS.html

[Return to top]

Water Sector

20. *February 26, Las Vegas Review−Journal* — **Nevada water timetable speeds up. Spurred by the region's record drought, the Southern Nevada Water Authority is accelerating its plans to develop more than one billion dollars worth of wells and pipelines connecting Las Vegas to water resources in rural Nevada.** On Thursday, the water authority board will discuss a report from staff that details plans to tap groundwater in Clark, Lincoln and White Pine counties and surface water rights the authority owns on the Virgin and Muddy rivers. The plan calls for three water projects to be built over the next 10 years. Using pipelines that would branch into northeastern and northwestern Clark County, bisect Lincoln County and stretch as far north as Ely, the largest of the three projects could increase the water supply for the Las Vegas Valley by as much as 200,000 acre−feet, two−thirds of its annual allotment from the Colorado River system. An acre−foot of water amounts to 325,829 gallons, enough to cover one acre of land with one foot of water. According to water authority figures, the average household in the Las Vegas Valley consumes about 230,000 gallons of water per year.
Source: http://www.reviewjournal.com/lvrj_home/2004/Feb−25−Wed−2004/news/23296430.html

[Return to top]

Public Health Sector

21. *February 26, Imperial College London* — **Capturing cell protein production could help fight antibiotic resistance.** The fight against antibiotic resistance could be aided by new 3D images of the final steps involved in manufacturing proteins in living cells, scientists say. By refining a technique known as cryo−electron microscopy, researchers from Imperial College London and CNRS−Inserm−Strasbourg University have determined how the enzyme RF3 helps prepare the protein−making factory for its next task following disconnection of the newly formed protein strand. **The team's success in capturing the protein−making factory, or ribosome, in action using cryo−electron microscopy will help scientists to begin deciphering the molecular detail of how many antibiotics interfere with the final steps of protein synthesis, an area not currently targeted in antibiotics research.** "Many antibiotics kill bacteria by interfering with their protein−making factories, or ribosomes. But bacteria can often become resistant by mutating their ribosome machinery. Observing ribosomes in action helps us understand which areas of the protein complex evolve such resistance quickly. This information could then be used to develop new antibiotics that target the more stable regions," said Marin van Heel of Imperial College.
Source: http://www.innovations−report.com/html/reports/life_sciences /report−26242.html

22. *February 26, BBC News* — **Superbug deaths increase.** The number of deaths involving the hospital superbug methicillin−resistant Staphylococcus aureus (MRSA) has soared in the United Kingdom over the last decade, official figures reveal. **Deaths from MRSA from 51 in 1993 to 800 in 2002. The UK Office of National Statistics said cases of MRSA increased from 210 to 5,309 over the same period.** Experts said the rise was partly due to better surveillance, but that more cases of MRSA were being seen. The latest statistics emerged from an Office of National Statistics and Health Protection Agency study. Researchers looked at thousands of death certificates from 1993 to 2002 which mentioned any kind of Staphylococcus aureus. They then went through them to see how many mentioned MRSA, the drug−resistant form of the infection, as a direct or contributing cause of death.
Source: http://news.bbc.co.uk/1/hi/health/3488946.stm

23. *February 25, USA Today* — **Universal flu shots considered. A panel of vaccine experts will explore for the first time the possibility of recommending annual flu vaccinations for all Americans.** Annual vaccination is advised for health workers and those considered at high risk of severe illness or death from flu, a total of 185 million people. Yet, nothing near that number has ever received flu vaccine. In the flu season now ending, little more than 83 million people were vaccinated. Keiji Fukuda of the U.S. Centers for Disease Control and Prevention, who spoke at a meeting of the Advisory Committee on Immunization Practices in Atlanta, said a subcommittee will begin gathering data on universal vaccination. **A recommendation for universal flu vaccination every year would improve overall vaccination rates, boost vaccine supply, and prepare the public health system for mass vaccinations if a flu pandemic strikes, he said.**
Source: http://www.usatoday.com/news/health/2004−02−24−flu−usat_x.ht m

24. *February 25, Canadian Press* — **CDC director says emergence of SARS, avian flu the new normal.** The flurry of exotic infectious diseases that have threatened global health in the past couple of years aren't an aberration, they are the new reality, the director of the U.S. Centers for Disease Control and Prevention (CDC), Julie Gerberding, said. **The rapid−fire emergence of**

diseases like Severe Acute Respiratory Syndrome (SARS), West Nile virus, monkeypox, and avian influenza point to a future where new and serious health threats arise on a regular basis from nature, Gerberding said in an interview. "We are living in a new normal," Gerberding told The Canadian Press. "The old days where an infection might emerge every now and again and capture our attention really has changed. These infections are on the move. And that's really, I think the major challenge."
Source: http://www.canada.com/health/story.html?id=E001A2B0−4AE1−400D−AFEC−105228A1B5F2

25. *February 23, Reuters* — **U.S. startled by extent of West Nile in blood donors. More than 1,000 blood donors have tested positive for West Nile virus in the United States, making the mosquito−borne disease one of the most common illnesses that can be acquired through transfusions, the U.S. Centers for Disease Control and Prevention (CDC) said on Monday, February 23.** "It is rather shocking," Lyle Petersen, a West Nile virus expert with the CDC, said in a telephone interview on the opening day of the American Mosquito Control Association's annual meeting. Petersen said the infected blood had been weeded out of the blood supply by new screening tests introduced in the U.S. last summer. "The screening has substantially improved the safety of the blood supply, but the risk is not zero," Petersen said. Almost two dozen Americans caught the virus from transfusions in 2002.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=4418486

[Return to top]

Government Sector

26. *February 26, Federal Computer Week* — **Analysis skill needed, experts say. A state homeland security director said state and local governments lack expertise in intelligence analysis to disseminate good counterterrorism information to public safety officials, but it may just be a question of training.** "Analysis is a very sophisticated intelligence skill set that resides primarily in the federal government, FBI, [the Defense Department], etc.," said Dennis Schrader, Maryland's homeland security director. "And we're going to try to build some of that capability in Maryland to be able to do the analysis, because without the analysis, the information is really useless." The federal government has experts who can turn information into intelligence, but it's hard to transfer those skills to state governments, Schrader said. Professional development for public safety officials would likely fill the gap, he added. **Schrader was one of several panelists at AFCEA (Armed Forces Communications and Electronics Association) International's homeland security conference in Washington, DC.** Although they touched on a number of subjects −− including interoperability, standards and partnering with industry −− many people said better intelligence and information sharing is needed for state and local public safety officials.
Source: http://www.fcw.com/geb/articles/2004/0223/web−afcea−02−25−04 .asp

[Return to top]

Emergency Services Sector

27. *February 27, The Nation (Bangkok, Thailand)* — **Authorities stage test run of emergency drills for subway.** Fire fighters, relief and rescue workers, bomb handlers, police dogs, explosives disposal experts, and representatives from the electricity, waterworks and telephone systems all gathered at Bangkok's Chalerm Ratchamongkon maintenance center Thursday, February 26, for a test run of emergency procedures on the new subway. Methods of handling emergencies such as fire, explosion and hostage−taking were tested. The new subway system is equipped with closed−circuit television and gas detectors. **Among the safety precautions designed into the subway system are an absence of garbage containers that could be used for hazardous materials and gates that open only after the cars stop.** Every gate is equipped with a sensor to detect whether an object or person has been caught in the gate.
Source: http://nationmultimedia.com/page.news.php3?clid=3&id=109024& usrsess=1

28. *February 26, Morning Journal News (Lisbon, OH)* — **Hazardous materials spill closes Ohio Route 14.** A portion of state Route 14 between the Pennsylvania state line and Ohio state Route 170 was closed for several hours Wednesday after a semi−truck carrying a hazardous material leaked. According to officials, a passer−by alerted the truck driver that fluid was escaping from the overflow valve in the tanker. The fluid was reportedly styrene polyester resin. The truck is owned by Manfredi Motor Transit Co., of Neville Island, PA. It was loaded with the liquid material at the Ashland Chemical Co. in Neville Island en route to Massillon, OH. **According to East Palestine Fire Chief Bret Todd, when the truck slowed for the red light on Route 14, the fluid shifted forward and a malfunction in the vapor release valve allowed the fluid to escape. Approximately 10−20 gallons leaked. Residents in about 15 homes were advised to stay inside of their homes until the material was cleaned up. The vapors from the fluid are hazardous, but the chilly temperatures Wednesday morning stopped that from being a problem.** An official from the Public Utility Commission of Ohio and an officer from the Motor Carrier Transport Enforcement Division of the Ohio State Highway Patrol were also at the scene investigating the matter.
Source: http://www.morningjournalnews.com/story.asp?ID=23905

29. *February 26, Click2Houston* — **Texas firefighters called to bomb scare.** A man was charged Wednesday, February 25, after he allegedly told a security guard near the Texas Medical Center in Houston that he had the makings for a "dirty bomb," officials told News2Houston. David O'Dell Ferguson, 54, was charged with making a terroristic threat, a Class A misdemeanor. But prosecutors said it was not because of what he said, but because of what he was carrying. Officials said around 9 p.m. Wednesday, Ferguson drove up to a guard at a Shamrock gas station on West Holcombe and Main and asked for directions to a FBI headquarters. According to police, he told the guard he wanted to turn in some chemicals that could be used to build a dirty bomb. "He used the right terminology so we had to take him seriously," Houston Police Department Sgt. L.P. Boutte said. "He named mercury, sulfur, and some kind of acid. If you mix those together, it could be caustic." **Houston police, bomb squads and hazmat crews responded to the scene and said they found mercury in its natural state inside the suspect's vehicle. No other materials were found. "The bomb squad came out and found out the suspect was in possession of about five ounces of mercury," Boutte said.** Houston police told News2Houston the suspect mentioned "dirty bombs" and was knowledgeable about the ingredients needed to make them.
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=46&id=26716

[Return to top]

Information and Telecommunications Sector

30. *February 26, Webuser (UK)* — **New version of Netsky worm appears. A new version of the Netsky worm has been detected that snares internet users by disguising itself as pornography or documents about hacking or MP3s. Once one of these files is opened, the Netsky.C infects the user's computer and sends a copy of itself to e−mail addresses on the infected computer. It can also spread via file sharing networks such as Kazaa and the ICQ chat system.** According to security experts, Netsky.C is similar to its predecessor Netsky.B as both spread by e−mail and file sharing networks. When it spreads via e−mail it selects random names for the subject line and file name. When first run, Netsky.C copies itself to the Windows folder as winlogon.exe and creates the following registry entry: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ICQNet= \winlogon.exe −stealth', so that winlogon.exe is run automatically each time Windows is started. Netsky.C also copies itself to folders on drives C to Z whose name contains the sequence of letters 'Shar', this includes shared folders and explains how it spreads through P2P file sharing where users download from each others' shared folders.
Source: http://www.web−user.co.uk/news/48008.html

31. *February 26, Federal Computer Week* — **Security trade group formed. Eleven computer security companies announced the formation of an advocacy group, the Cyber Security Industry Alliance, to influence public policy and spending on cybersecurity. The members, which include well−known computer security firms, said they want to promote generally accepted information security principles, exchange cybersecurity threat information with government agencies, and eventually expand education and research to improve cybersecurity.** Paul Kurtz was named executive director of the new organization. He is a former special assistant to the president and senior director of the Critical Infrastructure Protection Directorate under the White House's Homeland Security Council. Companies in the alliance are also interested in and supportive of the federal government's information technology product and systems certification program known as the National Information Assurance Partnership, said Ron Moritz, senior vice president and chief security strategist at Computer Associates International Inc.
Source: http://www.fcw.com/fcw/articles/2004/0223/web−security−02−26 −04.asp

32. *February 26, Vnunet.com* — **Security vendor mass−mails worm to clients. Antivirus firm F−Secure has apologized for sending the Netsky.B virus to several thousand of its UK customers and partners via a mailing list.** The e−mail apology said: "Because of a human error, you may have received an email infected with the Netsky.B virus that was relayed through our external email list server and was resent to our UK mailing list. The virus did not originate from our network −− it was sent by an unknown party to the list address. If you had up−to−date antivirus installed, the virus has been stopped automatically already and no further steps are necessary on your part." **Mikko Hypponen, F−Secure's director of antivirus research, said the mailing list was outside of the firm's normal e−mail scanning.** The Netsky.B worm spreads itself in e−mails inside a .zip archive or as an executable attachment. It also copies itself to shared folders of all available drives. This allows the worm to spread through peer−to−peer and local networks.

Source: http://www.vnunet.com/News/1153081

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_MYDOOM.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 3127 (mydoom), 20168 (−−−), 445 (microsoft−ds), 80 (www), 1434 (ms−sql−m), 137 (netbios−ns), 1080 (socks), 3128 (squid−http), 3072 (csd−monitor) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

33. *February 25, Associated Press* — **Interpol sets up new IT system. Interpol is setting up a new alert system to warn police of trends in disguising bombs and weapons −− like guns hidden in cell phones −− and other potential threats, the head of the international police organization said. Called Orange Notices, the computer−delivered alerts would keep Interpol's 181 member nations up to date on rapidly changing techniques and technologies used around the world.** "By checking orange notices, law enforcement people will have a better idea of what is coming at them," Interpol Secretary General Ronald Noble said. The orange alerts, the first change in the series since 1946, will offer more general advisories without necessarily naming suspects. The new program, still awaiting final approval for members, would join Interpol's new I−24/7 program to link law enforcement officers through a virtual private network on the internet. New York City's police department will soon be the first U.S. law enforcement agency to go on line, Noble said. So far, he added, 80 countries are being added to the system.
Source: http://australianit.news.com.au/articles/0,7204,8785941%5E15321%5E%5Enbv%5E15306,00.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. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

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

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nicc@dhs.gov or call (202)323−3204.

DHS/IAIP Disclaimer

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. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.