



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 23 February 2004

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
[For info click here](#)
www.whitehouse.gov/homeland

Daily Overview

- The San Mateo Daily Journal reports San Jose police have arrested the ringleader and the last of the 14 suspects who worked as waiters and waitresses at restaurants around the San Francisco Bay Area, specifically to steal credit card information from clients. (See item [5](#))
- The Washington Post reports the Department of Treasury has ordered banks to freeze the accounts of the Oregon and Missouri branches of the Saudi charity, al-Haramain Islamic Foundation, that U.S. officials say has been used to finance the al Qaeda terrorist network around the world. (See item [6](#))
- Reuters reports the Texas Animal Health Commission said a flock of chickens has tested positive for the H5N2 strain of avian influenza; this is the fourth U.S. state to be affected by the disease. (See item [14](#))

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 22, Mobile Register (AL)* — Security level increase is urged for LNG tankers. The federal government needs to raise the terrorist threat level in Boston to "high" every time a liquefied natural gas (LNG) tanker enters the city's harbor, say members of the Massachusetts congressional delegation. In a February 3 letter to Department of

Homeland Security Secretary Tom Ridge, the delegation described the LNG terminal at Everett, MA, as a "vulnerable target," and argued that federal funds should be used to cover the costs of protecting the tankers as they transit through the harbor. Protective measures during tanker transits include strongly armed police surrounding the harbor, snipers atop bridges and a Coast Guard presence replete with gunships. Tankers visit the Boston Harbor terminal once a week. During the orange alert last December, imposed because of concerns about imminent terror action against the United States, government officials delayed the arrival of an LNG tanker to Everett until they could intensify security at Boston Harbor. Both Massachusetts and Boston–area municipalities were eligible to be reimbursed by the federal government for extra costs incurred during that orange alert. Normally, when the threat level is lower than orange, neither local communities nor the state receive compensation for their LNG security expenditures.

Source: http://www.al.com/news/mobileregister/index.ssf?/base/news/1_077445387170050.xml

2. *February 20, Associated Press* — **Electric industry says grid audits due soon. Audits of the most critical areas of the nation's power grid will be completed by the end of June in hopes of avoiding the problems that caused last summer's blackout, the head of an industry group said Thursday, February 19. The North American Electric Reliability Council also promised that the industry will better disclose violations of reliability standards by grid operators and take aggressive action to correct them.** Michehl Gent, president of the industry–sponsored council said 20 audits will cover the centers where grid operators coordinate and control 80 percent of the power flowing through the system. The greatest focus is on the kind of problems responsible for the outage that affected eight states and parts of Canada in the August 2003. They include failing to trim trees, poor communications and equipment failures. The council will require faster reporting of violations of reliability rules by grid operators. The group, in a change, will report the violations to state or federal regulators if they are not promptly corrected.

Source: <http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20040220/NEWS08/402200347/-1/NEWS>

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

3. *February 19, InformationWeek* — **Army begins Active Directory rollout. The U.S. Army is in the early stages of implementing what will likely be one of the largest implementations of Microsoft's Active Directory technology.** Following a test period, the Army has begun building a directory that will help its system administrators manage user accounts for up to 500,000 Windows PCs. The upgrade will give the Army greater control over its IT resources and help it establish standard software configurations, says Dan Gilbert, senior Active Directory specialist with a contractor involved in the project. The Army expects to increase the

security of its IT infrastructure in the process. **The Army will be incorporating software that will make it possible to isolate a group of user accounts, or domain, if that group should be compromised by an intruder or mishap.**

Source: <http://www.informationweek.com/story/showArticle.jhtml?articleID=17701629>

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

Banking and Finance Sector

4. *February 20, Australian Associated Press* — **Organized crime groups target banks. Australian financial institutions are participating unwillingly in money laundering activity, with billions of dollars going undetected, business services firm KPMG said. KPMG Forensic Hong Kong director Nicholas Robinson said Australia was a target for money launderers, organized criminals and terrorist financing groups because its banking system worked well.** While KPMG said it was not possible to estimate how much money went undetected, they said the figure could be up to US\$6 billion, based on estimates for fraud-related activities of around US\$2 billion and money relating to drug trafficking of between US\$2 to US\$4 billion. Late last year the Australian government endorsed new global anti-money laundering standards issued by the Financial Action Taskforce on Money Laundering (FATF), a 33 member international body of which Australia is a member. The government announced it would proceed with a fundamental overhaul of Australian legislation. It also said it would set new standards for customer due diligence requirements for financial institutions, and extend anti-money laundering obligations to non-financial business and professions such as real estate agents, accountants and legal professionals.
Source: <http://www.smh.com.au/articles/2004/02/20/1077072842778.html>
5. *February 20, San Mateo Daily Journal (CA)* — **Credit card scam ring busted. An identity theft crime ring centering on California restaurant and its customers was cracked this week. San Jose police arrested the ringleader and the last of the 14 suspects who worked as waiters and waitresses at restaurants around the San Francisco Bay Area specifically to steal credit card information from clients.** When a customer paid by credit card, the employee would use a device to "skim" the credit card information from the magnetic stripe on the back of the card. The employees would then sell the credit card numbers to other members of the group; the other suspect would then manufacture a counterfeit credit card using the victim's account information. Police are not releasing the name of the restaurant. The waiter at the restaurant in question managed to steal \$13,000 over a period of just a month, Belmont police Sgt. Pat Halleran said. "The restaurant has been victimized," Halleran said. "These people were using their jobs there to steal." **San Jose police uncovered losses of about \$400,000 involving victims in California, Nevada, Utah and Washington.**
Source: <http://www.smdailyjournal.org/article.cfm?issue=02-20-04&storyID=28291>
6. *February 20, Washington Post* — **U.S. freezes accounts of large Saudi charity. The Department of Treasury ordered banks on Thursday, February 19, to freeze the accounts of the Oregon and Missouri branches of a large Saudi charity that U.S. officials say has been used to finance the al Qaeda terrorist network around the world. FBI and Internal Revenue Service agents searched a home in Ashland, OR, that is the U.S. headquarters for the charity, the al-Haramain Islamic Foundation.** The search is part of an investigation

into allegations that the Oregon branch was involved in money laundering and income tax and currency-reporting violations, Treasury officials said. Al-Haramain's headquarters in Saudi Arabia launched its Oregon office in 1997 by funding the work of an Ashland landscaper, Pete Seda, who had been sending Korans to prison inmates. The two people now mainly under investigation are Seda and Soliman Albuthe, a Saudi citizen who also helped run the Oregon organization. Officials are investigating numerous financial transactions involving Albuthe and Seda, also known as Pirouz Sedaghaty, including allegations of transporting large sums of undeclared traveler's checks across U.S. borders.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A55875-2004Feb 19.html>

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

Transportation Sector

- 7. *February 22, Houston Chronicle* — Ships collide; five missing. The U.S. Coast Guard is searching for five crew members of a Galveston-based offshore supply vessel that sank Saturday, February 21, after colliding with a larger ship in the Mississippi Delta. The accident remains under investigation, but fog may have been a contributing factor, a Coast Guard spokesman said.** The Lee III, owned by Galveston-based Ocean Runner Inc., collided with Zim Mexico III about 5:30 a.m. eight miles south of Pilot Town, LA, where the Mississippi River empties into the Gulf of Mexico. The ships rammed each other in the Southwest Pass, the main shipping lane from the Gulf of Mexico leading up the Mississippi River. The Lee III, a 178-foot offshore-platform supply ship, carried at least 30,000 gallons of diesel fuel, which may have leaked, said Petty Officer 3rd Class Jonathan McCool. The Lee III had left Venice, La., for the Gulf before the accident. **The channel was closed after the collision, Coast Guard officials said.** Investigators are assessing possible environmental damage and safety conditions connected to the leaking fuel. The Zim Mexico III, which sails under an Antigua flag, is owned by B. Rickmers GMBH&CIE and operated by ZIM-American Israeli Shipping Company Inc.

Source: <http://www.chron.com/cs/CDA/ssistory.mpl/nation/2414477>

- 8. *February 20, The Post and Courier (Charleston, SC)* — South Carolina Ports Authority seeks to levy security fee on ships. South Carolina ports officials want incoming ships to share the cost of security by adding a first-in-the-nation surcharge of \$1 per foot of a ship's length.** State Ports Authority President and CEO Bernard Groseclose said the charge, which could take effect as early as July, is necessary because of the rising costs of inspecting cargo and guarding the waterfront. **Industry watchers say such a fee could hamper South Carolina's competitiveness, possibly forcing shipping lines to look elsewhere in the Southeast to avoid paying several hundred dollars while sitting in port.** An estimated 2,300 barges and ships docked in the state's ports last year, ranging in size from a few hundred feet in length to almost 1,000 feet long. Bryan Blalock, general manager for APM Terminals in Charleston, which is part of Maersk Inc., said the add-on would cost the Charleston operation hundreds of thousands of dollars a year because of the number of 800-foot ships the company brings in annually. "It would be a significant impact as far as cost," Blalock said, adding that many area shipping companies are just starting to voice their concerns about the proposal.

Source: http://cnni.w.yellowbrix.com/pages/cnniw/Story.nsp?story_id=47325642&ID=cnniw&scategory=Transportation:Shipping&

9. *February 20, CNN* — **Moroccan flight diverted over domestic dispute. A domestic dispute — not suspected terrorism as early reports suggested — apparently led to the diversion of a Moroccan jet to Maine after it left a New York airport, government sources said Friday, February 20.** The Royal Air Maroc Boeing 767 resumed its journey to Casablanca, Morocco, at 3:51 a.m. ET Friday, according to an official at Maine's Bangor International Airport, where the plane landed Thursday night after the airline received a tip that a bomb could be aboard. But a government source in Washington wrote the entire episode off to a domestic dispute involving a married couple. "He left; she wanted to find him," the source said. The FBI took Zubair Ghias, 27, a Chicago stockbroker who "was identified as possibly having a bomb," off the plane in Bangor and rescreened the remaining passengers, the FBI spokesman said. Osterrieder said that Ghias told a story of kidnapping when questioned. Reported missing by his wife since Saturday, Ghias alleged he had been abducted then, the FBI said.
Source: <http://www.cnn.com/2004/US/Northeast/02/20/diverted.flight/index.html>

10. *February 20, Reuters* — **Report highlights world travel risks.** For many international business travelers preoccupied with getting the job done, safety and security concerns may cover only the obvious — theft and assault. **But today's world climate poses far more serious challenges, some of which are touched on in a new report listing the 10 countries most at risk for terrorism. Listed not by degree of risk but alphabetically, they are Colombia, Indonesia, Israel, Kenya, Pakistan, the Philippines, Russia, Saudi Arabia, Turkey and Yemen.** That compilation comes from iJET Travel Risk Management, a company that sells security, intelligence, safety and health information to corporations and individual travelers covering more than 450 worldwide destinations. Nigeria, Spain and Thailand have been removed from the list because of anti-terrorism steps taken by those three countries. They have been replaced, however, by three others — Pakistan, Saudi Arabia and Turkey.
Source: <http://www.cnn.com/2004/TRAVEL/02/20/biz.trav.travel.risk.report/index.html>

11. *February 20, Department of Homeland Security* — **Secretary of Homeland Security Tom Ridge announces enhanced security along the Mexican border. Department of Homeland Security Secretary Tom Ridge and the Mexican Secretary of the Interior Santiago Creel today, February 20, agreed on significant border safety and security initiatives in bilateral meetings in Mexico City.** These agreements preserve the free flow of \$630 million in trade across the U.S./Mexico border every day while maintaining the integrity of the border. The United States and Mexico further agree to jointly and vigorously fight alien smuggling rings and to prosecute those who perpetrate these crimes. **"We are dedicated to one goal: to protect the American and Mexican people from the threat of terrorism," said Secretary Ridge following the meeting.** Secretary Ridge reaffirmed President's Bush statement on Mexican President Vicente Fox's State Visit in September 2001 that "We have no greater friend than Mexico and our commitment never wavered."
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0352.xml

[[Return to top](#)]

Postal and Shipping Sector

12.

February 21, Associated Press — **Man charged with hacking post office Web server.** A 21-year-old Minneapolis, MN, man who allegedly hacked into a Web server belonging to the U.S. Postal Service has turned himself in to federal agents and faces computer fraud charges. The U.S. attorney says the man was indicted on two counts of computer fraud and one count of possessing 15 or more unauthorized access devices. **The grand jury alleged that the man transmitted a code in May 2002 that damaged a Web server database table owned by the U.S. Postal Service's office of inspector general.**

Source: http://www.kare11.com/news/news-article.asp?NEWS_ID=59863

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

Agriculture Sector

13. *February 21, Associated Press* — **Bioterrorism rules delay elk testing. Federal rules classifying the bacteria *Brucella abortus* as a potential bioterrorism weapon have delayed attempts to determine the cause of a disease outbreak in Wyoming cattle.** *Brucella abortus*, one of several *Brucella* species, was classified a "select agent" following the September 11, 2001, terrorist attacks. When a Sublette, WY, cattle herd tested positive for the disease in December, ranchers and livestock officials suspected the Muddy Creek elk feedground near the ranch. Earlier tests showed a 29 percent brucellosis exposure rate among the feedground elk. Wyoming wildlife researchers had to leave a bacteria sample from an aborted fetus, found in 2002 on the Muddy Creek Feedground, in the freezer because of federal rules. New bioterrorism regulations require researchers to handle "select agents" in approved "select agent labs."

Source: <http://www.billingsgazette.com/index.php?tl=1&display=rednews/2004/02/21/build/wyoming/47-brucellosis.inc>

14. *February 20, Reuters* — **Texas finds bird flu on poultry farm.** A case of the bird flu virus was found on a poultry farm in Texas, the fourth U.S. state to be affected by the disease, state government officials said on Friday. **The Texas Animal Health Commission said a flock of chickens in Gonzales County tested positive for the H5N2 strain of avian influenza, a milder version of the potentially deadly disease.** Texas becomes the fourth U.S. state in two weeks to be affected by bird flu. Delaware, New Jersey, and Pennsylvania have also reported mild strains of the virus. Texas officials said it did not appear that bird flu had spread from the East Coast states into Texas. More than 20 countries have banned imports of some or all U.S. poultry. Russia, the top U.S. poultry buyer, earlier on Friday placed a temporary ban on Texas chickens even before it was publicly announced.

Source: http://www.agriculture.com/worldwide/IDS/2004-02-20T163449Z_01_N20403956_RTRIDST_0_BIRDFLU-TEXAS-UPDATE-1.html

15. *February 19, Reuters* — **U.S. livestock ID program to begin this year.** A national livestock identification system will begin to be put into effect this year, one of the government's responses to the first U.S. case of mad cow disease, a senior U.S. Department of Agriculture (USDA) official said. **Scott Charbo, USDA's chief information officer, said he would make recommendations to Agriculture Secretary Ann Veneman in coming months on the shape of the animal ID system.** Open questions include whether the system will be mandatory and how costs will be shared, if at all, he said in remarks at the USDA's annual outlook forum.

Charbo began looking at options soon after the December 23 discovery of the nation's first case of mad cow disease. Veneman directed Charbo to oversee an acceleration of adoption of a tracking system that could trace within 48 hours the history of livestock as a step to protect food safety and animal health in the event of a disease outbreak. **There are one million farms, ranches and feedlots that produce livestock and 2,000 slaughterhouses, according to USDA, so creation of an ID system will be a massive task. One-half of the cow-calf operators have no animal ID system at all, according to USDA data.** "We are looking at some type of phased implementation," Charbo said. "We believe there will be some implementation in 2004 and 2005 as well."

Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=goDe tail_ANewsindex_html_51334_1

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

Food Sector

16. *February 20, Food and Drug Administration* — **Guacamole recalled. Fresh Foods Concepts, Inc., is recalling Trader José's Fresh Guacamole and Senior Felix's Guacamole because they have the potential to be contaminated with Listeria monocytogenes.** Listeria is a common organism that can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with a weakened immune system. The affected products were sold on or after Friday, February 13, 2004, at Trader Joe's stores and Whole Foods outlets throughout Southern California. No illnesses have been reported to date in connection with this problem. **The recall was initiated after an avocado pulp sample from an outside supplier tested positive for Listeria.** Production and distribution of this product have been suspended while the company and the Food and Drug Administration investigate the source of the problem.

Source: http://www.fda.gov/oc/po/firmrecalls/freshfood02_04.html

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

Water Sector

Nothing to report.

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

Public Health Sector

17. *February 20, Associated Press* — **Asia's bird flu strikes house cats. Bird flu has jumped to new species in Asia, killing three house cats and infecting a white tiger in Thailand, officials said Friday.** The pet cats in Nakhon Pathom province outside Bangkok are the first domesticated mammals known to have contracted the disease in the current outbreak. Thai veterinarian Teeraphon Sirinaruemit also said a white tiger at Khao Khiew zoo near Bangkok was found to have the virus, but it has since recovered. The developments came as the head of the UN Food and Agriculture Organization urged international cooperation in fighting the disease, warning it could spread to more animals. The virus has killed at least 22 people in

Thailand and Vietnam, while infecting birds in 10 Asian nations. A World Health Organization (WHO) official said it's possible that Indonesia could have human cases despite government claims to the contrary. "It's such a large country and such a large population ... it may have been diagnosed as ordinary pneumonia," the WHO official, Georg Petersen, said. **The infection of three cats in Thailand has raised fears that the disease could spread from pets to humans, WHO virus expert Prasert Thongcharoen said.** Health experts are concerned about the bird flu sickening other animals, in part because that could prompt mutations in the virus that in turn could make it easier to pass among people.

Source: http://news.yahoo.com/news?tmpl=story2&cid=541&u=/ap/20040220/ap_on_he_me/asia_bird_flu_6&printer=1

18. *February 20, Voice of America* — **WHO launching anti-polio campaign in 10 African nations.** The World Health Organization (WHO) says it will begin a large-scale polio immunization campaign next week in 10 African countries, as an outbreak from Nigeria spreads across the region. **The WHO says tens of thousands of volunteers will go house to house starting on Monday, with the goal of vaccinating 63 million children. It says polio is again spreading across west and central Africa, paralyzing children in seven countries that had been free of the virus.** The WHO has linked the outbreak to several northern Nigeria states, where Islamic leaders have refused to immunize children over fears the vaccine is contaminated with substances that can cause AIDS, cancer, and sterility. The agency's regional director for Africa, Ebrahim Samba, says the African continent is on the brink of reinfection unless immunization campaigns stop the polio virus from spreading. Polio usually infects children through contaminated drinking water. It attacks the central nervous system, causing paralysis, deformity and, in some cases, death.

Source: <http://www.voanews.com/article.cfm?objectID=10CD7E78-516E-4805-9F85150B71A940A4>

19. *February 19, CNN* — **Researcher isolated after possible Ebola exposure. A civilian Army researcher at Fort Detrick, MD, is in isolation after possibly being exposed to the Ebola virus, Army officials said Thursday.** The researcher accidentally pricked herself with a needle that contained a weakened form of the Ebola virus last week while she was injecting mice with the virus as part of a research effort. **The woman has shown no signs of the illness, but will remain at Fort Detrick for up to 30 days of isolation.**

Source: <http://www.cnn.com/2004/HEALTH/02/19/ebola.exposure/>

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

Government Sector

Nothing to report.

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

Emergency Services Sector

20. *February 20, Federal Computer Week* — **Border patrol trains on Range 3000.** Since the beginning of January, federal border patrol agents in southern Texas have been training

on an advanced interactive firearms simulator tailored to unique confrontations they face. "Our work is not metropolitan," said Agent Rey Diaz, public affairs officer with the McAllen Sector of the U.S. Bureau of Customs and Border Protection. "We don't work in the city. We don't work on the highways. The majority of our work is out in the brush, out in desolate areas. So the scenarios have to be specifically tailored to situations the border patrol agent would encounter being on his own or with his partner." The simulator — also used by the FBI, the Coast Guard, the Transportation Security Administration and the U.S. Federal Protective Service — depicts stressful scenarios agents could encounter, such as suspects with weapons. Users stand in front of a large projection screen with untethered weapons and act — including using verbal commands — just as they would in real life. Such training, say advocates, helps law enforcement officials make better decisions in stressful situations. About 1,500 agents patrol 17,000 square miles, including 284 river miles. So far they have created 15 different scenarios for the simulator, Diaz said.

Source: <http://www.few.com/few/articles/2004/0216/web-simul-02-18-04.asp>

21. *February 20, Government Computer News* — **NOAA: Rescues rising with satellite beacons. Satellite beacons have already led rescuers to save the lives of 34 people in life-threatening situations this year, the National Oceanic and Atmospheric Administration (NOAA) said. Last year, NOAA helped rescue 224 people who activated beacons on land, sea or in the air.** The Federal Communications Commission last July approved public use of pocket-sized personal locator beacons, or PLBs. People who buy them either new or used must by law register them in the National 406-MHz Beacon Registration Database, said SARSAT program manager Ajay Mehta. Delays caused by unregistered signals "may be the difference between life and death," Mehta said. NOAA also requires registration updates every two years, or whenever the data changes. When activated by someone in distress, a beacon sends its location to rescue authorities via NOAA satellites and the Search and Rescue Satellite Aid Tracking System, SARSAT. NOAA's geostationary and polar-orbiting operational environmental satellites receive the 406-MHz signals from three types of beacons: Emergency position-indicating radio beacons, or EPIRBs, for maritime rescue Emergency locator transmitters, or ELTs, for aviation use PLBs for land use.

Source: http://www.gcn.com/vol1_no1/daily-updates/25032-1.html

22. *February 19, Government Technology* — **Gov. Wise awards funds to purchase amateur radio equipment for first responders.** West Virginia Gov. Bob Wise recently awarded \$50,000 to the Kanawha County Commission to purchase amateur radio equipment for the new Ned Chilton 911 Center and the Kanawha County Unified Mobile Command Post. **"Amateur radio operators are some of the first on the scene to help establish communication in an emergency," Wise said. "This funding will help our first responders continue the wonderful job they do to protect us every moment of every day."** The radio equipment will be used in the Emergency Operations Center at the Ned Chilton 911 Center, where emergency resources and public-safety response are coordinated in times of emergency, and in the Kanawha County Unified Mobile Command Post.

Source: <http://www.govtech.net/news/news.php?id=89492>

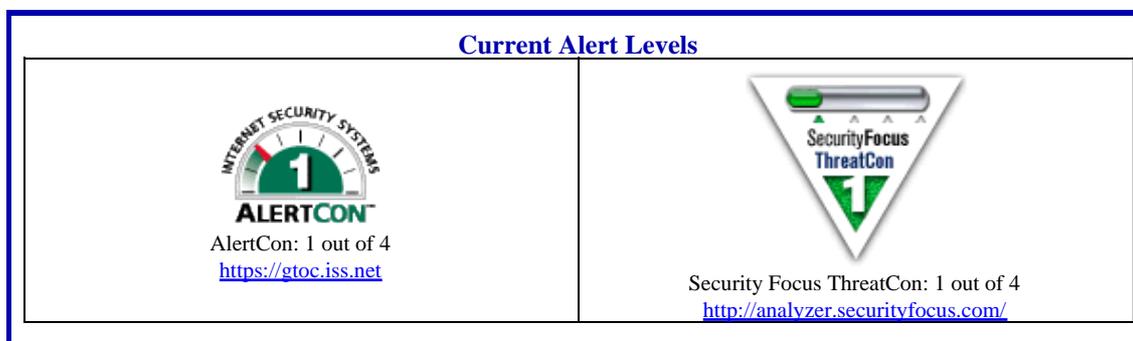
[\[Return to top\]](#)

Information and Telecommunications Sector

23. *February 20, eWeek* — **ZoneAlarm bug bares system to e-mail attack.** Security vendor Zone Labs has disclosed that several versions of its personal-firewall products are vulnerable to a buffer-overflow attack. ZoneAlarm, ZoneAlarm Plus and ZoneAlarm Pro 4.0.0 versions; ZoneAlarm Pro 4.5.0; as well as Zone Labs Integrity Client 4.0.0 are vulnerable. ZoneAlarm users are advised to upgrade to Version 4.5.538.001. The problem was described by eEye Digital Security on the BugTraq mailing list. The firewalls process SMTP (e-mail) traffic sent to or from the system. According to the description, a sufficiently large value in the SMTP "RCPT TO" command can overflow a stack-based buffer in the TrueVector Internet Monitor (vsmon.exe) process. According to Zone Labs, **"If successfully exploited, a skilled attacker could cause the firewall to stop processing traffic, execute arbitrary code, or elevate malicious code's privileges."** An attacker with local access and restricted privileges could invoke the attack by sending an e-mail with the overflowed RCPT TO command. The user could elevate his privileges to SYSTEM level, and a remote user could invoke the attack by manipulating the system into sending an e-mail with the overflow value. Additional information available here: <http://download.zonelabs.com/bin/free/securityAlert/8.html>
Source: <http://www.eweek.com/article2/0.4149.1530946.00.asp>

24. *February 18, SearchSecurity.com* — **Sun combats security holes in cancelled Cobalt line.** Sun Microsystems continues to battle operating system vulnerabilities in its doomed line of Cobalt appliance servers. **Administrators should upgrade to prevent remote exploits that could include cracking private keys, exposing confidential data, spoofing identities, escalating privileges, executing arbitrary code and denial of service.** Perhaps the most serious vulnerability is a heap-based buffer overflow in rsync. Remote attackers can use this to gain access to a system or execute arbitrary code. Sun has fixes for RaQ 550, Qube 3 and RaQ 4. A defect in gnupg incorrectly creates El Gamal sign and encrypt keys using the same key component. This could allow an attacker to get the private key from a signature, which could be used to spoof identities and decrypt confidential data. Fixes are available for Qube 3, RaQ 550 and RaQ XTR. An integer overflow in the ls program in the fileutils or coreutils packages can render applications that use ls, including wu-ftpd, vulnerable to remote exploitation. Attackers could cause a denial of service on the server. There are fixes for RaQ XTR, RaQ 550, Qube 3 and RaQ 4. Finally, an update is available for an unspecified vulnerability in IPtables on RaQ 550.
Source: http://searchsecurity.techtarget.com/originalContent/0,28914,2,sid14_gci950995,00.html?track=NL-358

Internet Alert Dashboard



Current Virus and Port Attacks

Virus:	#1 Virus in the United States: WORM_LOVGATE.G 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	3127 (mydoom), 135 (epmap), 445 (microsoft-ds), 80 (www), 1434 (ms-sql-m), 1433 (ms-sql-s), 137 (netbios-ns), 1080 (socks), 3128 (squid-http), 389 (ldap) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

25. *February 22, Telegraph (United Kingdom)* — **Britain's MI5 to recruit new agents. The budget of MI5, Great Britain's internal intelligence agency, is to be raised by 50 percent to pay for 1,000 extra agents in a new onslaught against terrorism.** David Blunkett, the Home Secretary, will announce on Wednesday that the budget for the intelligence services will rise from \$2 billion to almost \$2.8 billion. Most of the extra money will go to MI5, while the budgets for MI6 and GCHQ, the Government's listening center, will be increased only in line with inflation. MI5, which is based at Millbank in central London beside the Thames, has about 2,100 staff. This is expected to rise to more than 3,000 by October. The sharp increase in the number of MI5 spies will be the central feature of the biggest shake-up of the security services since the Second World War. **It will make MI5, which specializes in threats to Britain internally, one of the biggest and most well resourced security services in the world.** Blunkett has decided to increase funding after a two-year review of the services.

Source: <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2004/02/22/nspook22.xml&sSheet=/portal/2004/02/22/ixportal.html>

26. *February 22, Associated Press* — **Haitian rebels seize government's last bastion.** Rebels have seized the government's last major bastion in northern Haiti. Now, there's celebrating in the port city of Cap-Haitien — and looting. Some people are shooting off celebratory rounds in the air, while several others looted and torched buildings. **Rebels in the city center say they met little resistance except at the airport. There, they say eight people were killed in fighting with militant civilians loyal to President Jean-Bertrand Aristide.** One rebel boasted that "we came in today and we took Cap-Haitien, tomorrow we take Port-au-Prince," the capital.

Source: <http://www.nbc6.net/news/2865378/detail.html>

27. *February 20, CNN* — **Nuclear scandal: Man confesses.** Malaysian police say a Dubai-based businessman has confessed to helping a top Pakistani scientist sell nuclear secrets and supplies to Iran and Libya. **February 20's report of the confession by Buhary Syed Abu Tahir came a week after U.S. President George W. Bush named the 44-year-old Sri Lankan as the middleman representing Abdul Qadeer Khan — the father of Pakistan's nuclear bomb — in his black market network.** Now, according to a detailed report released Friday by Malaysian police, Tahir — who has residency status in Malaysia — said Khan sold nuclear parts to Iran for about \$3 million in cash, and he served as the middleman. Tahir

also told Malaysian authorities that Khan had arranged for enriched uranium and centrifuge units to be sent directly by air from Pakistan to Libya in 2001–02. He also named several businessmen from Germany, Turkey, Switzerland and the United Kingdom as part of the "loose network" of middlemen that helped procure the nuclear equipment for Khan. Since Khan's February 4 shock confession that he transferred Pakistan's nuclear weapons secrets to other countries, authorities around the world — from Pakistan to China to Malaysia — have been working to uncover the full extent of the network.

Source: <http://www.cnn.com/2004/WORLD/asiapcf/02/20/nuclear.malaysia/index.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 Assessments, 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 nipc.watch@fbi.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.