



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 05 December 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports President Bush has signed into law a measure to fight identity theft: the Fair Credit Reporting Act, which sets a national credit reporting standard to make it easier for people to monitor their credit ratings and to get credit cards, loans and mortgages. (See item [5](#))
- The Associated Press reports a federal grand jury has indicted 41 people for allegedly buying and selling fraudulent commercial driver's licenses that could be used to transport people, weapons, chemicals or other hazardous materials that could be used in terrorism. (See item [18](#))
- VNUNet reports that firms using Cisco's Aironet access points running Cisco IOS operating software are vulnerable to a security flaw that allows hackers to gain full access to wireless networks. (See item [24](#))

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. *December 04, Reuters* — Opec to hold production steady. OPEC oil producers agreed on Thursday to keep oil supplies on hold for the winter and move aggressively to shore up high world crude prices early next year. OPEC kept output limits unchanged at 24.5 million

barrels a day and will meet again on February 10 in Algiers, UAE Oil Minister Obaid bin Saif al-Nasseri said. **OPEC, which controls half the world's crude trade, says it expects to cut deliveries in February.** Producers already appear to have a consensus on the need for tougher restraints than as demand eases after the northern winter and to make room for the recovery in post-war Iraqi exports. Kuwaiti Oil Minister Sheikh Ahmad al-Fahd al-Sabah said that at least one million barrels daily, four percent of group supply, would need to be removed. U.S. light crude eased by 55 cents to \$30.55 a barrel. For the United States, rising crude prices could mean extra heating oil and gasoline costs.

Source: <http://edition.cnn.com/2003/BUSINESS/12/04/opec.oilprice.reu.t/>

2. *December 03, Reuters* — **Louisiana pipeline explosion, leak. The U.S. Coast Guard said on Wednesday it is investigating two pipeline incidents in the Gulf of Mexico off the Louisiana coast.** In the first incident, a dredging boat struck the Gulf South Natural Gas Pipeline in the Atchafalya Basin about 39 miles south of Morgan City, LA, causing an explosion and fire on Tuesday. The fire was quickly extinguished, the Coast Guard said in a statement. In a separate incident, a leak from an Exxon Mobil Corp. crude oil pipeline was spotted by a Coast Guard helicopter flying on Tuesday over Bartaria Bay, about six miles south of Grand Isle, LA, the Coast Guard said. Exxon Mobil shut the pipeline after being notified.

Source: <http://www.forbes.com/markets/newswire/2003/12/03/rtr1167949.html>

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

3. *December 03, Federal Computer Week* — **Pentagon renovation goes forward.** The product manager of information technology systems for the Pentagon Renovation Program said it will be the largest upgrade ever for the 60-year-old building that houses the Department of Defense (DoD). Renovation plans were originally scheduled to be complete in 2015, but Congress pushed the deadline up to 2010 and increased funding by \$300 million. **The two largest projects at the moment involve consolidating thousands of disparate servers around the building into one centrally-managed server farm and developing a single command center for each of the armed services, rather than have them run their own command centers,** Hari Bezwada said at the E-Gov Homeland Security conference in Washington, DC. The building already has 100,000 miles of telephone line, and it will get between 700,000 and one million miles of data lines over the next seven years. **After the September 11, 2001, terrorist attack on the Pentagon, DoD officials upgraded the systems in the damaged wedge.** Less than a year after, the wedge re-opened with fiber cables and the beginnings of a single network backbone that Bezwada said will eventually spread throughout the entire Pentagon. Additional information available on the Pentagon Renovation Program Website:

<http://renovation.pentagon.mil/>

Source: <http://fcw.com/fcw/articles/2003/1201/web-pentagon-12-03-03.asp>

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

Banking and Finance Sector

4. *December 04, IT–Analysis* — **The growing problem of identity theft.** According to the 2003 Computer Crime Survey conducted by the Computer Security Institute in conjunction with the FBI, **nearly 13% of respondents had been the victim of identity theft in the past year in the U.S.** In total, **losses from identity theft in the U.S. in the past year are estimated to have amounted to around \$50 billion.** As the use of the Internet has grown, so too have the incidences of online identity theft. Theft of credit card and account information is one of the most common reasons for identity theft, but consumer liability is generally capped in the case of such fraud — leaving financial institutions to pick up the pieces. According to MasterCard, identity theft accounts for 7% of all fraud committed and is a growing problem. Further, fraud committed during card–not–present transactions accounts for 60% of fraud. Until recently, identity theft has been less of a threat in Europe than in the U.S. One of the reasons why it has been such a problem in the U.S. is the traditional use of social security numbers as an identifier. However, **the UK Home Office estimates that identity theft is growing at 165% per year in the UK and is currently costing the country \$2.2 billion annually. Furthermore, the areas in which identity theft is growing fastest are Eastern Europe and Southeast Asia — two of the new hotspots in the current spate of outsourcing.**

Source: <http://www.it-analysis.com/article.php?articleid=11489>

5. *December 04, Associated Press* — **Bush signs measure to fight identity theft. Americans will be able to get free copies of their credit histories every year and will gain new weapons against identity thieves under legislation President Bush signed into law on Thursday.** The legislation renewed the Fair Credit Reporting Act, which set a national credit reporting standard to make it easier for people to get credit cards, loans and mortgages. Without reauthorization by Congress, the act would have expired. Under the legislation, consumers will be able to e–mail, call or write the three major credit bureaus for a free copy of their credit report and their credit score each year to help them understand why their credit was denied or approved. The law requires businesses to black out Social Security numbers, parts of credit card numbers and debit card numbers on receipts, and require the coding of medical information on credit reports. **The law also creates a national system of fraud detection so that identity theft can be traced quickly. Until now, victims of identity theft have had to call credit card companies to shut down their accounts, and the three major credit rating agencies to report the crime and protect their credit rating.**

Source: http://abcnews.go.com/wire/Politics/ap20031204_1731.html

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

Transportation Sector

6. *December 04, The Patriot News (Harrisburg, PA)* — **Rules will put brakes on truckers' workdays.** A new federal law that will limit the hours truck drivers can work is designed to make the highways safer. **But trucking companies and shippers are scrambling to deal with**

the changes, which they say could cost them money. Some also say they will have to hire more drivers, which will put more big rigs on the road. The new rules require truck drivers to stop working for 10 consecutive hours each day, among other changes. The government projects that 1,326 fatigue-related crashes will be avoided, saving up to 75 lives a year. Opponents and proponents agree that the new rules represent a tremendous change for the trucking industry. **The new rules, which take effect January 4, are being issued by the Federal Motor Carrier Safety Administration. The so-called "Hours of Service" rules have been in effect since 1939, and this is the first major revision to be adopted.** The revisions allow for 11 hours of driving time. But drivers can only be on duty for 14 hours, which includes time spent on breaks, loading and unloading. Under the new rules, drivers cannot extend their workday by taking breaks.

Source: http://pennlive.com/news/patriotnews/index.ssf?/base/news/10_70533987132490.xml

- 7. December 04, Associated Press — Ferry crash investigation expanding.** The probe into the fatal crash of New York's Staten Island ferry is expanding to include senior officials. **Two law enforcement sources said federal prosecutors are examining the actions of the director of ferry operations and other workers in the city Department of Transportation. The probe will look at whether safety rules were properly enforced. The case could be presented to a grand jury within weeks.** Ten people were killed and dozens injured when the off-course ferry plowed into a concrete pier in October. The ship's pilot said he passed out at the controls, and witnesses say the ship captain was not in the wheelhouse when the ferry came in to dock.

Source: <http://www.turnto10.com/news/2679999/detail.html>

- 8. December 04, KDKA TV (Pittsburgh) — Deputy in trouble over airport breach.** An Allegheny County sheriff's deputy is in trouble with the law after a bizarre security breach at Pittsburgh International Airport. **According to federal authorities, Deputy Eddie Rose had his girlfriend pose as a handcuffed prisoner and tried to pass her through security checkpoints so she wouldn't have to wait in a long line at the airport.** Sources told KDKA Investigator Marty Griffin that Rose called in sick from work on Tuesday, then put on his uniform and went with his girlfriend to the airport. At the airport, Rose reportedly draped a jacket over her wrists to make it appear as though she was in handcuffs, flashed his badge and told screeners he was transporting a prisoner. Though the pair made it past the screeners, Allegheny County police became suspicious and stopped them, asking for the so-called prisoner's name. When questioned, Rose reportedly admitted that the woman was his girlfriend and that he was trying to help her avoid waiting in line. **Meanwhile, the Transportation Security Administration is charging Rose with "trying to circumvent a security system."** The incident is under investigation.

Source: http://kdka.com/local/local_story_338095457.html

- 9. December 04, UPI — Plan assists Mexican trade.** Department of Homeland Security Secretary Tom Ridge is expected to announce Thursday, December 4, a system to allow commercial trucks to clear customs at the Mexican border in as little as five seconds by using preregistered ID cards. A similar system has had success regulating trucks from Canada, but the less-secure southern border could pose challenges. "We actually have gone through an enrollment program of enrolling drivers, carriers and the companies that import goods," U.S. Customs official Jayson Ahern said recently at an industry homeland security conference. **Under the new program, trusted truckers, trucking companies, manufacturers and**

importers will be screened, investigated and registered for expedited crossings. When enrolled trucks approach the border, information about their identification and contents will already have been transmitted electronically so they "can actually travel through the borders without impediment on our part," Ahern said. "We want to make sure that all the legal traffic and all the good stuff that is supposed to come through doesn't get bogged down," Martin Rojas, director of cross-border operations at the American Trucking Association, said in an interview yesterday. "We want to be sure that we can keep that balance of facilitation and enforcement."

Source: <http://washingtontimes.com/national/20031203-103254-9162r.htm>

10. *December 03, Department of Transportation* — **U.S. Transportation Secretary Mineta announces \$2.85 billion federal down payment to restore mass transit in lower Manhattan. U.S. Transportation Secretary Norman Y. Mineta on Wednesday announced \$2.85 billion in transit funding for Lower Manhattan, the first down payment on the Bush administration's commitment to restoring mass transit in Lower Manhattan in the aftermath of the September 11, 2001, terrorist attacks.** "The important thing for all taxpayers and the Lower Manhattan recovery is that these funds are available as needed for the grantee to expedite the development and completion of these critical public transportation projects," said Secretary Mineta. The federal funding for these grants will be available this week. Secretary Mineta was joined by New York Governor George E. Pataki and New York Mayor Michael R. Bloomberg for the announcement, which took place at the temporary PATH (Port Authority Trans Hudson) Station at Ground Zero in New York. "**President Bush and I remain committed to rebuilding Lower Manhattan and strengthening the transportation infrastructure that was destroyed by the September 11, 2001, terrorist attacks,**" Secretary Mineta said. "These grants will help commuters get to their homes and work more quickly, and restore the efficiency of New York City's mass transit system."

Source: <http://www.dot.gov/affairs/fta5103.htm>

[[Return to top](#)]

Postal and Shipping Sector

11. *December 03, Datamonitor* — **DHL is resuming its flights to Iraq and Afghanistan.** DHL Express has decided to resume operations in both Iraq and Afghanistan, just a week after the company had cancelled all flights in the region. **DHL suspended services in Iraq after one of its planes was hit by a surface-to-air missile and was forced to make an emergency landing after it took off from Baghdad airport.** The incident put the company on alert and, after reassessing the security situation in the region, DHL stopped flights to Afghanistan as well. DHL announced Tuesday that it had resumed flights in the region after being advised that it is now a safe environment to fly in. **The company added it was introducing security measures to prevent further attacks.** DHL is not the first express and cargo carrier to consider implementing extra security measures in light of increased worldwide instability following the September 11 attacks. DHL's rival FedEx set up its own police force to fight terrorism last October. DHL carries post and parcels to and from US soldiers, as well as packages for aid organizations in Iraq.

Source: http://www.commentwire.com/commwire_story.asp?commentwire_ID=5110

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

Agriculture Sector

12. *December 04, Ohio Ag Connection* — IBDV boosts campylobacter numbers in chickens.

Ohio State University scientists have found that infectious bursal disease virus (IBDV) can increase the number of dangerous campylobacter growing in broilers. **"What we've found is that in chickens infected with bursal disease that become immuno-suppressed, the number of campylobacter (organisms) present in the gut is much higher than in birds that haven't been immuno-supressed,"** said Daral Jackwood, with the Food Animal Health Research Program at the Ohio Agricultural Research and Development Center (OARDC). **"Campylobacter doesn't hurt chickens, but it causes disease in humans."** Campylobacter jejuni is the most common cause of foodborne illness and bacterial diarrhea in the United States. **According to the U.S. Centers for Disease Control and Prevention, an estimated 2.1 million to 2.4 million cases of campylobacteriosis occur each year in the nation.** Jackwood's study has shown that IBDV contributes to the growth of campylobacter in young chickens in the laboratory. Next, he will examine flocks in the field to see if they experience the same increase.

Source: <http://www.ohioagconnection.com/story-state.cfm?Id=87&yr=2003>

13. *December 03, Animal and Plant Health Inspection Service* — USDA establishes

biotechnology environmental unit. The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) Wednesday announced the creation of an environmental and ecological analysis unit within its biotechnology regulatory services (BRS) program. APHIS has had a strong focus on analyzing the environmental and ecological effects of genetically engineered plants. **This new unit will provide additional resources to address anticipated increases in permit applications to field test genetically engineered plants and petitions to deregulate these products.** This staff will ensure that as science advances, all the necessary safeguards are in place to protect agricultural and natural resources. The new unit will also help APHIS expand its environmental analyses as it considers new regulations under the Plant Protection Act of 2000. **Employees in this unit will conduct analysis of the environmental and ecological effects of field testing genetically engineered plants to assist in the development of BRS regulations and permit conditions, ensure BRS' continued compliance with environmental regulations and coordinate oversight of BRS' environmental impact statements.**

Source: http://www.aphis.usda.gov/lpa/news/2003/12/biounit_brs.html

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

Food Sector

14. *December 03, Food and Drug Administration* — FDA and CBP bolster safeguards on imported food. The Food and Drug Administration (FDA) and the U.S. Customs and Border Protection (CBP) Wednesday signed a memorandum of understanding (MOU) that allows FDA to commission thousands of CBP officers in ports and other locations to

conduct, on FDA's behalf, investigations and examinations of imported foods. This unprecedented FDA–CBP collaboration significantly strengthens the implementation of the Bioterrorism Act to assure the security of imported foods. The MOU upgrades the two agencies' teamwork in training, day–to–day operations, and information sharing. **As part of the MOU, FDA can commission all the CBP officers the two agencies consider necessary to conduct examinations and investigations in accordance with the FDA's recently issued interim final rule requiring prior notice of food imported or offered for import to the United States.** FDA and CBP will provide specialized training for the commissioned CBP employees who will carry out this work, and both agencies will expand their existing cooperative arrangements to directly share information affecting the safety and security of imported foods. The MOU goes into effect immediately and is available online:

<http://www.fda.gov/oc/bioterrorism/moucustoms.html>

Source: <http://www.fda.gov/bbs/topics/NEWS/2003/NEW00988.html>

[[Return to top](#)]

Water Sector

Nothing to report.

[[Return to top](#)]

Public Health Sector

15. *December 04, Associated Press* — **New Mexico officials confirm hantavirus case.** New Mexico health officials have confirmed the first case of hantavirus in the state since June 2001. A 37–year–old Rio Arriba County woman hospitalized at the University of New Mexico Hospital has the pulmonary disease, the state Department of Health reported Wednesday. **The New Mexico office of epidemiology is conducting an environmental investigation to determine potential exposure sites. The news brings New Mexico's total number of hantavirus cases to 60 since the illness was discovered in the Four Corners area in 1993, the Health Department said.** People contract the disease when they breathe dust contaminated by an infected rodent's urine, feces or saliva. The disease cannot be spread by person–to–person contact. Thirty–eight percent of those who contract the disease die from it. **Nationwide, 353 cases have been confirmed with 132 deaths, according to the U.S. Centers for Disease Control and Prevention.**

Source: http://abcnews.go.com/wire/Living/ap20031204_1115.html

16. *December 04, Scientist* — **European CDC closer to reality. European health ministers have agreed in principle to create a European Center for Disease Prevention and Control (ECDC), whose goals would be similar to those of the U.S. Centers for Disease Control and Prevention (CDC).** The health ministers, meeting in Brussels as part of the European Council, approved guidelines for creation of an ECDC similar to those suggested in July by the European Commission. The ECDC's prime focus would be to provide a structured and systematic approach to the control of communicable diseases and other serious health threats, including potential bioterror attacks. **The ECDC would become operational in early 2005 with a staff of about 30 people, growing eventually to a full force of only about 100 people.**

Core tasks of the ECDC would include epidemiological surveillance and laboratory networking, early warning and rapid and effective response to health threats, providing scientific assessments, providing technical assistance and investigative teams in Europe or outside of Europe, development of EU level preparedness planning for health crises, and communicating on health threats.

Source: <http://www.biomedcentral.com/news/20031204/04/>

17. *December 03, Associated Press* — **CDC report: U.S. not ready for SARS.** The United States is ill-equipped to handle a major outbreak of the Severe Acute Respiratory Syndrome (SARS) virus, according to a report commissioned by the U.S. Centers for Disease Control and Prevention (CDC). The study, conducted by University of Louisville researchers, cites a lack of specialists who study diseases, along with cuts in state and local health department budgets. **"The current shortage of epidemiologists, public health nurses and other personnel in the U.S. will reach a crisis stage in the event of an epidemic," the report says. "If these positions are not restored, an otherwise containable epidemic may spread rapidly."** Though the most recent SARS epidemic was contained, health officials say it could re-emerge any time, possibly aided by an expected worse-than-normal flu season. The report recommends the U.S. develop more capacity in hospitals for a surge in people quarantined for SARS and clearly delineate authority and responsibility among federal, state and local agencies. The report, "Quarantine and Isolation: Lessons Learned from SARS," is available online: <http://www.instituteforbioethics.com>
Source: <http://www.cnn.com/2003/HEALTH/12/03/sars.report.ap/>

[[Return to top](#)]

Government Sector

18. *December 04, Associated Press* — **Forty-one charged for fake licenses. A federal grand jury has indicted 41 people for allegedly buying and selling fraudulent Utah commercial driver's licenses.** Of the 41, three — Wade William Higbee, Wendy Dawn Prescott and Ricardo Rosas Salazar — face multiple federal counts of making a false certificate of driver competency, for allegedly forging the certification documents that allowed the others to obtain the licenses from the state. The scheme was discovered more than a year ago during an internal audit by the Utah Driver's License Division of third-party testers, Department of Public Safety Commissioner Robert Flowers said. A third-party tester is someone who conducts the certification tests for those seeking a commercial driver's license, usually to operate large 18-wheel trucks, and then signs the supporting documents that must be presented to the state before a license is issued. The audit showed an inordinate number of licenses were being issued by certain testers, Flowers said. A closer look, including a cross-check of the names of license-seekers with Social Security numbers, indicated fraud and prompted the investigation, he said. **Law officers were concerned about the scheme for its potential threat to homeland security, Flowers said. Commercial vehicles could be used to transport people, weapons, chemicals or other hazardous materials that could be used in terrorism.**
Source: <http://www.casperstartribune.net/articles/2003/12/04/news/wyoming/c5ddc8fa627b889a87256df2005a1bac.txt>

[[Return to top](#)]

Emergency Services Sector

19. *December 04, Highland Park News (Chicago)* — **Firefighters spend time training with hazardous materials.** Highwood, Highland Park, and Glencoe firefighters completed three days of training exercises for hazardous material spills using a 9,000-gallon tanker truck donated by Exxon-Mobil Corp. "We practice decontamination and handling incidents," said Highland Park Deputy Chief Alan Wax. **The practice session used an empty tanker but did involve the use of foam and other safety equipment. The tanker helps firefighters become familiar with valves and placement of equipment around an actual vehicle. The company provided the tanker and three instructors who showed firefighters how the tanker is designed and how it works.** About 55 firefighters, Wax said, were able to train. "Everybody I talked to said it was a good drill," said Highwood Fire Chief Thomas E. Lovejoy. "It's not an ordinary training experience." **Wax said the fact that Skokie Valley Road and a railroad freight line go through Highland Park requires firefighters know hazardous material control techniques.**

Source: <http://www.pioneerlocal.com/cgi-bin/ppo-story/localnews/curr ent/hp/12-04-03-163564.html>

20. *December 04, Click2Houston* — **Texas 911 dispatch system back online.** The \$53 million Houston Emergency Center computer system crashed again Friday. **Officials reported the system back online by 12:30 p.m. Friday after being offline since approximately 8:30 a.m. This is the center's fourth crash. News2Houston reported that Houston police and firefighters were all inconvenienced by the outage. After the system went back online, News2Houston heard a police officer receive a 5-hour-old call for police from a citizen.** "All these people are trying to get police service and can't. That's not right," Officer Johnnie McFarland said. McFarland, who is also a member of the Fraternal Order of Police, said he is worried that an officer, firefighter or citizen will be killed during one of the outages. **The city has acknowledged the new system's troubles since the day it went online. But Friday's outage was the first time the system went down for more than one hour.** Workers dispatched all calls manually and took records by hand while the city worked with the software vendor to correct the problem. News2Houston reported that some police dispatchers were delaying calls, telling officers in the field that non-emergency calls would have to wait until the system was fixed. Officials have not determined what caused the system to crash.

Source: <http://cms.firehouse.com/content/article/article.jsp?section Id=17&id=22549>

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

Information and Telecommunications Sector

21. *December 05, Mercury News (CA)* — **Tech firms urged: secure cyberspace.** Department of Homeland Security (DHS) Secretary Tom Ridge warned Wednesday, December 4, that terrorists who "know a few lines of code can wreak as much havoc as a handful of bombs." It is important that "we share information, work together and close any gaps and weaknesses that terrorists would otherwise seek to exploit," Ridge told an audience of about 350 business leaders and technology experts attending the National Cyber Security Summit in

Santa Clara, CA. "It only takes one vulnerable system to start a chain reaction that can lead to a devastating result," Ridge added. Robert Liscouski, the DHS's assistant secretary for infrastructure protection, made clear there would be consequences if the corporations that control 85 percent of the nation's critical infrastructure chose not to cooperate. **The DHS wants businesses to provide information about cyber attacks so it can identify major threats to computer networks that control everything from water supplies and power lines to banking and emergency medical services. DHS officials say they need such data to create an early warning system.** The full text of Secretary Ridge's remarks are available on the DHS Website: http://www.dhs.gov/dhspublic/interapp/speech/speech_0151.xml
Source: <http://www.bayarea.com/mld/mercurynews/business/7410944.htm>

22. December 04, — Industry groups release security tools. A pair of information technology industry groups unveiled security assessment tools at this week's National Cyber Security Summit in Santa Clara, CA. TechNet, an association of chief executive officers (CEO) and other senior executives, unveiled its Corporate Information Security Evaluation tool, which takes CEOs, chief information officers, and chief security officers through 88 points on risk management, people, processes, and technology. The Information Technology Association of America, in partnership with the Marshall School of Business at the University of Southern California, announced its Cyber Security Assessment, which will build on information provided by the TechNet evaluation. The key is performing both assessments regularly and measuring progress at every step, said Harris Miller, president of ITAA. **Both tools drew from the government's recent experience with self-assessments under the Government Information Security Reform Act (GISRA) of 2000 and the Federal Information Security Management Act (FISMA) of 2002,** said Art Coviello, co-chairman of TechNet's Cyber Security CEO Task Force. There, the focus also was on repeated measurements to identify shortcomings and demonstrate improvement or regression, he said.

Source: <http://www.fcw.com/fcw/articles/2003/1201/web-summit-12-04-03.asp>

23. December 04, Federal Computer Week — Fed cybersecurity chiefs get a council. Information security has become important enough to warrant a federal Chief Security Officers Council to work with similar groups of government executives, the man in charge of national cybersecurity said this week. There is already a CIO Council, a CFO Council and a Chief Human Capital Officers Council, but security is so complicated now that Amit Yoran, director of the Department of Homeland Security's National Cyber Security Division, decided to initiate a council focused specifically on that one issue. "The CIOs have a lot on their plate and under [the Federal Information Security Act] every agency must have a security official...and this allows them to collaborate and discuss issues," Yoran said. **The new CSO Council will work closely with the CIO Council, but having a separate forum where chief security officers can get together and discuss problems, tactics and best practices should make improvement easier,** Yoran said.

Source: <http://fcw.com/fcw/articles/2003/1201/web-council-12-04-03.a.sp>

24. December 04, VNUNet (UK) — Cisco issues wireless Lan security alert. Cisco has warned firms using its Aironet access points running Cisco IOS operating software of a security flaw that allows hackers to gain full access to wireless networks. The vulnerability allows hackers to steal Wired Equivalent Privacy (Wep) encryption keys. The issue arises if the wireless Lan device's 'SNMP-server enable traps wlan-wep' command is enabled. "Under

these circumstances, an adversary will be able to intercept all static Wep keys," Cisco said in a statement. If the command is switched on, which Cisco stressed is disabled by default, the access point will broadcast any network static Wep keys in cleartext to the SNMP server every time a key is changed or access points rebooted. **Affected hardware models are the Cisco Aironet 1100, 1200 and 1400 series.** Cisco has posted a workaround advising companies with deployments of these devices to disable this command, adding that any dynamically set Wep key will not be disclosed. **The problem only applies to wireless Lan kit running its IOS software**, so Aironet access point models running VxWorks are not affected. Customers are advised to upgrade their IOS version to a patched system. Cisco's advisory and workaround are available here: <http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP-trap.shtml>
 Source: <http://www.vnunet.com/News/1151249>

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: JAVA_BYTVERIFY.A 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), 1434 (ms-sql-m), 137 (netbios-ns), 21 (ftp), 445 (microsoft-ds), 80 (www), 139 (netbios-ssn), 1433 (ms-sql-s), 4662 (eDonkey2000), 27374 (SubSeven) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

25. *December 04, Associated Press* — **Rocket blast near U.S. Embassy in Kabul. A rocket exploded in a field near the U.S. Embassy in Kabul on Thursday, about two hours after U.S. Defence Secretary Donald Rumsfeld met with Afghanistan's leader in another part of the capital.** A U.S. military official said Rumsfeld had safely left the country to continue his tour of Central Asia. No one was injured in the explosion, which one official blamed on fighters from Afghanistan's ousted Taliban rulers or their ally, renegade warlord Gulbuddin Hekmatyar. The rocket exploded in a military athletic field across the street from the embassy, witnesses said. As police and soldiers with flashlights searched the field where the rocket landed on a moonlit night, Kabul military commander Mohammed Ayub Salangi said they found a piece of

shrapnel that appeared to come from a truck-launched rocket. **Hekmatyar, a former prime minister, heads Hezb-e-Islami, a faction that fought Soviet Russian troops in Afghanistan in 1980s. He is suspected of having urged Afghans to fight the U.S. led coalition forces now in the country** and American forces are searching for him.

Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thes tar/Layout/Article_Type1&c=Article&cid=1070535736520&call_pa geid=968332188854&col=968705899037

26. December 04, Washington Post — Terror defendant gets ten year prison term. A Yemeni American who attended an al Qaeda training camp and met with Osama bin Laden shortly before the September 11, 2001, attacks was sentenced Wednesday, September 4, to 10 years in prison. Mukhtar al-Bakri, 23, is the first defendant to be sentenced in the Lackawanna Six case, which has been held up by the Bush administration as a model in pursuing and prosecuting terrorism suspects. Al-Bakri, the youngest member of the group, was the last to accept a plea bargain earlier this year. His sentence for providing material support to al Qaeda is expected to be among the harshest because he is one of only two who completed the camp's training program. He could have received 15 years if convicted at a trial. He was also fined \$2,000.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A33459-2003Dec 3.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 703-883-6631

Subscription and Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-6631 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.