

**Department of Homeland Security
Information Analysis and Infrastructure
Protection
Daily Open Source Infrastructure Report
for 09 May 2003**

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Sacramento Bee reports two years after an energy crisis repeatedly blacked out parts of the state and sent giant companies into bankruptcy, California's power market is still ripe for exploitation this summer. (See item [4](#))
- The Washington Post reports Montgomery County (Maryland) police and federal investigators said on Wednesday that a April 5 incident in Germantown was the key to unraveling one of the largest cases of identity theft and credit card fraud in the Washington, D.C. area. (See item [6](#))
- The Associated Press reports Microsoft has acknowledged the flaw that affected all of its 200 million Passport accounts, but said it had fixed the problem early Thursday morning. (See item [21](#))
- VOANews.com reports the U.S. completely rejects Iran's assertion of a peaceful nuclear program and will press for a finding by the International Atomic Energy Agency next month that Iran has violated the nuclear Non-Proliferation Treaty. (See item [27](#))

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. *May 07, Reuters* — **NRC plans safety revisions for U.S. nuke plants.** The U.S. Nuclear Regulatory Commission (NRC) on Wednesday proposed revising its labyrinth of rules for atomic power plants to make clear what equipment and safety systems should get top priority.

The NRC said current regulations cover a wide range of "structures, systems and components" at the country's 103 commercial reactors to ensure they can be safely shut down in the event of an accident. While some of the current facilities and systems "are very important to safety," others provide "minimal or a negligible contribution to safety," the NRC said in a statement. Nuclear power accounts for 20 percent of the electricity generated in the U.S. The new regulations are being weighed as the industry grapples with heightened security and safety concerns in the wake of the September 11, 2001 attacks on New York and the Pentagon and worries about the safety of the thick steel lids that cap pressurized water reactors. **Cracks in reactor vessel heads and leaks have been discovered at a handful of nuclear plants, prompting lengthy shutdowns and costly repairs. The NRC has issued new orders to tighten security at nuclear plants to thwart attacks and has stepped up reactor safety inspections.** It was not clear when the NRC will issue the revised regulations.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3827994

2. *May 07, Reuters* — **Deutsche Bank gets green light to trade power in United States.** Germany's Deutsche Bank said on Wednesday it had received a license to trade electricity in the U.S. market. Deutsche's move comes after UBS Warburg, the investment banking arm of Swiss bank UBS AG, bought the trading business of collapsed energy trader Enron Corp. "We received the license from the The Federal Energy Regulatory Commission (FERC) last week," Harriet Benson, spokeswoman at Deutsche Bank, told Reuters. No further details were immediately available. **Wall Street firms have shown interest in entering the risky but lucrative market in the U.S. Banks have also moved in to trade in the European power and gas markets.** Alongside traditional energy firms, they are expected to fill some of the gaps left by U.S. traders which quit the European energy market after the collapse of Enron.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3827398
3. *May 07, Newstream.com* — **Largest fuel cell deal ever. In the biggest sign yet that America may finally be ready to free itself from foreign sources of energy -- two giant industrial leaders have completed the largest ever hydrogen fuel cell deal.** According to the deal, General Motors will take the hydrogen that is a byproduct of Dow Chemical's manufacturing processes and use it with General Motors Fuel cells technology to create electricity. **While hydrogen is the most abundant element on the planet -- it needs to be refined.** A fuel cell captures electricity when pure hydrogen passes through a special membrane and combines with oxygen to create H₂O. **Individual stationary fuel cells have enough power for ten homes or a small business.** General Motors says, "make no mistake," their interest in fuel cells is ultimately for automotive applications -- and this deal, they say, will jump start us down the road to a hydrogen-based economy.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=newstream_2003_05_07_eng-newstream_eng-newstream_183116_8530338202551427396a
4. *May 07, Sacramento Bee* — **California's power grid vulnerable as woes go unresolved. Two years after an energy crisis repeatedly blacked out parts of the state and sent giant companies into bankruptcy, California's power market is still ripe for exploitation.** The state's grid operator predicts a new round of market manipulation could add \$50 million or more to annual electricity costs starting this summer. **Today, under a system that's only partly evolved beyond the chaos of the market meltdown, power generators can get paid**

handsomely to relieve transmission line congestion by pulling promised power off the system, even if they played a role in overloading it. "The thing that scared us the most about all this whole mess of the energy crisis is remarkably little has been done to deal with the underlying problems," said Michael Shames, head of the Utility Consumers' Action Network. The money involved is relatively small in a \$10 billion annual electricity market, but the game's existence is a sign that in the past two years, efforts to fix a flawed system have been hobbled by a deep schism over what solution best serves consumers. **Meanwhile, now that more power plants have been built, transmission line clogs are becoming more common, more difficult to manage and more vulnerable to trading schemes.**

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=sacbee_2003_05_07_eng-sacbee_news_eng-sacbee_news_083414_5383815443971511550.ewa>

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

5. *May 07, The White House* — **Personnel announcement – nominations for Secretaries of the Army and Navy. The President intends to nominate James G. Roche of Maryland, to be Secretary of the Army. He currently serves as Secretary of the Air Force.** Prior to returning to the Department of Defense in 2001, he served as Corporate Vice President and President of the Electric Sensors and Systems Sector of the Northrop Grumman Corporation where he served since 1984. Roche is a twenty-three year veteran of the U.S. Navy. **The President also intends to nominate Colin R. McMillan of New Mexico, to be Secretary of the Navy.** Currently, he is Chairman and CEO of the Permian Exploration Corporation. In March of 1990, McMillan was appointed by President George H. W. Bush to be Assistant Secretary of Defense (Production and Logistics). He served as Assistant Secretary until 1992, the same year he was honored by the Department with a Medal for Distinguished Services.

Source: <http://www.whitehouse.gov/news/releases/2003/05/20030507-8.h tml>

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

Banking and Finance Sector

6. *May 08, Washington Post* — **Huge credit scheme alleged card factory found in Md. home, police Say.** Montgomery County police and federal investigators said on Wednesday that a April 5 incident in Germantown was the key to unraveling one of the largest cases of identity theft and credit card fraud in the Washington area. **During an April 21 search of the home of Francis E. Fletcher Jr. and Michele Fletcher, police said, a veritable factory for counterfeit credit cards was found: 600 pages containing more than 40,000 allegedly stolen names and credit card numbers; more than 100 newly minted cards under 100**

different names, featuring the trademark Visa logo. The Fletchers have been arrested and charged with identity theft and theft of property over \$500, as well as conspiracy to commit those crimes. Their arrest was first reported Tuesday night by WRC-TV (Channel 4). Attempts to reach the couple, who posted \$100,000 bond each, were unsuccessful on Wednesday. Investigators said they believe the evidence may tie the Fletchers to hundreds of thousands of dollars of merchandise illicitly purchased in Maryland, Virginia and the District in the last two years. Other arrests may follow, authorities said, and they may present the case to the U.S. attorney to file federal charges.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A28116-2003May7.html>

7. *May 07, Times-Dispatch* — **Credit union responds to data hacking. Someone hacked into a merchant's computer system, compromising information on cards and leaving some bank and credit-union customers without use of cards with the Visa logo.** Virginia Credit Union responded by blocking the use of 800 Visa cards, canceling the accounts and issuing new account numbers and cards. New cards should arrive in the mail this week. **Visa said in a statement "We are currently working with law enforcement and our member financial institutions in this matter to ensure the protection of our cardholders,"** but declined to say how many institutions or cardholders were affected.

Source: <http://www.timesdispatch.com/business/MGB6S1MMEFD.html>

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

Transportation Sector

8. *May 08, The Christian Science Monitor* — **U.S. port security: Is X-ray enough?** Boston now scans two-thirds of the containers, making the port an exemplar of antiterror tactics. **Every year, 16 million containers move through America's 361 ports. Only 4 percent get scanned – leaving what may be the biggest hole in the nation's terror shield. In a sense, Boston's 70-percent scan rate makes it one of the most secure U.S. ports.** It also highlights a fundamental question now circling among port officials, political leaders, and the shipping industry: Would scanning more containers – even up to 100 percent – boost security? Even as the debate grows, security experts warn that scanning is only one component of effective seaport security. **A major upgrade in scanning would detain legions of containers at ports, making them more vulnerable to sabotage or tampering. It would also require thousands of new government inspectors and billions of dollars in salary and equipment costs. Ultimately, a more layered approach may be more effective – and cheaper.** For example, the customs bureau's new Container Security Initiative, under which lists of container contents are forwarded to U.S. authorities 24 hours before a shipment leaves a foreign port, gives officials time to assess the risk. **They can analyze the contents, the history of the container, and the boat it's traveling on. High-risk cargo is then marked for special scrutiny. Another key element is securing containers. Most "seals" are now quarter-inch-thick pieces of plastic and metal, and safer seals are being developed.**

Source: <http://www.csmonitor.com/2003/0508/p02s01-usgn.html>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

9. *May 08, Wisconsin Ag Connection* — **EC shows results of livestock electronic tag study. The European Commission (EC) has revealed the results of the IDEA (Electronic Identification of Animals) project, a study into tagging livestock.** The results of the extensive six–nation trial were shown on a farm near Rome, Italy and confirmed the feasibility of electronic tagging of cattle, sheep, and goats. The Commission said that conventional systems based on ear tags, tattooing and marking can be modified and are not always reliable, potentially rendering them ineffective. IDEA was a large–scale experiment running from March 1998 to December 2001. One million farm animals were electronically identified in six European Union countries: France, Germany, Italy, the Netherlands, Portugal, and Spain. The feasibility of various tagging systems for ruminants was explored and the structure needed to implement them was determined. **Taking into account the findings of the IDEA project, the Commission has submitted a draft proposal for a Council regulation "Establishing a system for the identification and registration of ovine and caprine animals."**

Source: http://www.wisconsinagconnection.com/story-national.cfm?Id=5_18t

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

Food Sector

10. *May 07, Government Computer News* — **Food safety agency uses new software.** The U.S. Agriculture Department (USDA) is using reporting software to get a hawk-eyed view of the nation's poultry, egg and meat processing plants. **Since November, the department's Food Safety and Inspection Service has been using a software application to give supervisors and other employees quick, detailed information on 6,500 meat, poultry, and egg processing plants.** About 300 of the service's employees are using the software, including 150 circuit supervisors, who use the software to create reports and graphs in seconds, said Peter Kuhmerker, director of the service's Field Automation and Information Management Division. Food inspection programs in 25 states also use the program, he said. **The service uses the software for a multitude of queries, such as identifying plants that have sanitation problems or high levels of noncompliance.**

Source: http://gcen.com/vol1_no1/daily-updates/22021-1.html

11. *May 06, Food and Drug Administration* — **FDA issues final two proposed food safety regulations. The U.S. Food and Drug Administration (FDA) announced Tuesday the publication of the final two food safety proposed regulations required by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, which gave FDA new authority to protect the nation's food supply.** The proposals are two of four proposed regulations that the Act calls upon FDA to develop regarding food safety. These two proposals deal with establishing and maintaining records among food firms, and the

administrative detention of foods that may pose a risk to public health. The recordkeeping proposal is designed to help FDA track foods implicated in future emergencies, such as terrorism-related contamination. **Under the proposed rule, manufacturers, processors, packers, distributors, receivers, holders and importers of food would be required to keep records identifying the immediate source from which they received the food, as well as, the immediate subsequent recipient, to whom they sent it. The other proposed regulation on administrative detention implements FDA's new authority to detain any article of food for which there is credible evidence that the article poses a threat of serious adverse health consequences or death.**

Source: <http://www.fda.gov/bbs/topics/NEWS/2003/NEW00902.html>

12. *May 05, National Institute of Neurological Disorders and Stroke* — **Pressure combined with heat reduces prion infectivity in processed meats. The combination of high temperature and very high pressure in the preparation of processed meats such as hot dogs and salami may effectively reduce the presence of infective prions while retaining the taste, texture, and look of these meats, according to a study.** The study was led by Paul Brown, M.D., of the National Institute of Neurological Disorders and Stroke (NINDS), a component of the National Institutes of Health within the U.S. Department of Health and Human Services. **Scientists believe that bovine spongiform encephalopathy, also known as "mad cow" disease, entered the human food chain through beef products containing abnormal, or folded, proteins called prions.** The disease manifests itself in humans as variant Creutzfeldt–Jakob disease. Since 1995 more than 140 patients, mostly in the United Kingdom, have died as a probable result of eating contaminated meat products. The combination of temperature and high pressure has been used commercially for the past 15 years to reduce the amount of bacteria in foodstuffs and to preserve ham, chicken, salsa, and other foods. **Dr. Brown said his team "took the process one step further, to see if it would kill prions, which it did."**

Source: http://www.ninds.nih.gov/news_and_events/pressrelease_prion_infectivity_050503.htm

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

Water Sector

Nothing to report.

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

Public Health Sector

13. *May 08, Technology Review* — **New DNA sensor. University of Rochester researchers have designed a simple, inexpensive sensor that can detect specific sequences of DNA on-the-fly.** The researchers' sensor chip contains hairpin-like stalks of DNA that straighten to expose fluorescent molecules attached to their ends when they combine with a given sequence of DNA. **The chip could eventually be used as a cheap, instant test for biowarfare agents and pathogens like strep throat bacteria, and could also be used in genetic screening, drug discovery, and forensics, according to the researchers. The method is sensitive enough**

that it does not require the usual, time-consuming step of making thousands of copies of a piece of DNA in order to have enough material to test. To use the chip, a scientist would place a drop of solution containing the DNA to be identified onto the chip and watch for a change of color.

Source: http://www.technologyreview.com/articles/rnb_050803_2.asp

14. *May 08, Associated Press* — **WHO extends SARS travel warning to Taiwan.** The World Health Organization (WHO) on Thursday extended a Severe Acute Respiratory Syndrome (SARS) travel warning to Taiwan and to two more Chinese provinces. **"WHO is now recommending as a measure of precaution that people planning to travel to Tianjin and Inner Mongolia provinces of China and Taipei in Taiwan consider postponing all but essential travel,"** said a statement by the U.N. agency. The agency has already issued travel warnings for Hong Kong, Beijing and China's Guangdong and Shanxi provinces.

Source: <http://apnews.excite.com/article/20030508/D7QT5SOG0.html>

15. *May 07, BBC News* — **Beijing deploys SARS investigators.** Thousands of Severe Acute Respiratory Syndrome (SARS) investigators have been deployed in the Haidian district of China's capital Beijing, which has been worst hit by the disease, in a desperate bid to stop its spread. **The 30,000 investigators will check businesses and residences throughout the area looking for victims and ensuring that measures are being taken to improve hygiene, district official Zhou Liangluo said. Each household in the district of 2.2 million people has been issued with a thermometer and emergency contact numbers, while offices and businesses have been ordered to install temperature-monitoring systems.** Prime Minister Wen Jiabao has warned that it is of vital importance to prevent the disease spreading in the country's rural areas where so far there has not been a large epidemic.

Source: <http://news.bbc.co.uk/2/hi/asia-pacific/3005921.stm>

[[Return to top](#)]

Government Sector

16. *May 08, U.S. Department of State* — **Visas: documentation of immigrants--victims of terrorism – Interim rule with request for comments.** This rule amends the Department's regulations concerning immigrant visas. Recent legislation, commonly known as the USA Patriot Act, permits certain victims of the September 11, 2001 terrorist attack to file petitions for classification as special immigrants. **This rule implements these provisions by creating a new visa classification ``SP'' for these immigrants and sets forth the eligibility requirements for the issuance of an immigrant visa in that category.** Effective date: This interim rule is effective on May 8, 2003. Comment date: The Department will consider written comments submitted on or before July 7, 2003.

Source: <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocke.t.access.gpo.gov/2003/03-11222.htm>

17. *May 07, National Institute of Standards and Technology* — **NIST reports on progress of WTC investigation at one-third mark– agency notes cooperation, seeks more information.** The National Institute of Standards and Technology (NIST) today made public its

second status update on the agency's federal building and fire safety investigation into the World Trade Center (WTC) disaster of Sept. 11, 2001. At a press briefing in New York City (NYC), NIST Director Arden Bement Jr. reported solid progress by the investigation team at the one-third mark of the ongoing 24-month effort and thanked the many private citizens and organizations who helped the team to date. **As part of its progress report, NIST has included an interim report that documents the procedures and practices used to provide the passive fire protection (fireproofing) for the floor system of the WTC towers. Nothing in the interim report—based on a review of factual data in documents obtained by NIST—should be taken to imply that the floor trusses played a critical role in the collapse of the WTC towers. The fireproofing issue is a key component of the ongoing NIST investigation.**

Source: http://www.nist.gov/public_affairs/releases/wtc05-07-03.htm

18. *May 07, Government Executive* — **Officials weigh 'unique challenges' of information sharing.** Officials from the Defense and Homeland Security departments on Wednesday described their ongoing efforts to achieve federal, state and local unity on data needed in the event of national disasters or terrorist attacks. **"The flow of information is getting better, but we've got some unique challenges,"** said Col. Charles Lewis, intelligence director at the Northern Command's joint task force for civil support. **He called getting information from domestic intelligence agencies in a timely manner the military's biggest challenge in fulfilling its role in domestic affairs.** Lewis spoke as part of a panel discussion at an Armed Forces Communications and Electronic Association event.

Source: <http://www.govexec.com/dailyfed/0503/050703td1.htm>

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

Emergency Services Sector

19. *May 08, Greensburg Daily News (Indiana)* — **Chemical problems in Indiana county.** The burning topic at Wednesday's quarterly meeting of the Local Emergency Planning Committee (LEPC) was hazardous materials. **Sulfuric acid, anhydrous ammonia and chlorine are among the many hazardous materials housed in Decatur County, according to literature handed out by Rand Hooton, chairman of the LEPC. "Locally, the majority of our chemical releases have been from minor anhydrous thefts," Hooton said. "The major concern is the release that could occur on the interstate from a breached semi."** Scott Chasteen, Greensburg firefighter, agreed. "We are prepared to handle the chemicals that are reported to exist in the county," he said. "The unknown chemicals traveling through are what's most dangerous." **The LEPC has received some help in fighting chemical spills through a pair of grants. The Decatur County Community Fund donated \$4,600 and the REMC added \$1,000 to be used for the purchase of decontamination equipment. "Any hazmat incident requires a clean-up,"** said Iris Wilhoit, director of the Emergency Management Agency.

Source: [http://www.greensburgdailynews.com/cgi-bin/LiveIQue.acgi\\$rec =44000?gb_story](http://www.greensburgdailynews.com/cgi-bin/LiveIQue.acgi$rec =44000?gb_story)

20. *May 07, KITV TheHawaiiChannel.com* — **Official impressed with Hawaii terrorism preparedness.** Assistant Secretary of Defense, Paul McHale, was on Oahu to see how various, city, state, federal and military first response teams would handle a biological or chemical

attack. "I was extraordinarily impressed with what I saw today. **Clearly folks in Hawaii, civilian and military have achieved a level of cooperation when it comes to homeland security and homeland defense that I have not seen anywhere else in the United States,**" McHale said. **McHale was at Schofield Barracks Tuesday to observe several agencies respond to a mock terrorist emergency. The first responders had to pretend a radioactive device was found at Fort DeRussy and about 150 people were exposed to it.** McHale said Hawaii's responders were quick, efficient, and cooperative. "Although the technology here in Hawaii is extraordinary, the military capabilities are significant, it really comes down to a matter of attitude," McHale said.

Source: <http://www.thehawaiichannel.com/news/2188854/detail.html>

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

Information and Telecommunications Sector

21. *May 08, Associated Press* — **Microsoft admits Passport was vulnerable.** Computer researcher Muhammad Faisal Rauf Danka of Pakistan discovered how to breach Microsoft Corp.'s security procedures for its Internet Passport service. **The service is designed to protect customers visiting some retail Web sites, sending e-mails and in some cases making credit-card purchases. Microsoft acknowledged the flaw affected all its 200 million Passport accounts but said it fixed the problem early Thursday,** after details were published on the Internet Wednesday night. Under a settlement with the Federal Trade Commission (FTC) last year over lapsed Passport security, Microsoft pledged to take reasonable safeguards to protect personal consumer information during the next two decades or risk fines up to \$11,000 per violation. The FTC's Jessica Rich said Thursday that **each vulnerable account could constitute a separate violation – raising the maximum fine that could be assessed against Microsoft to \$2.2 trillion.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A30330-2003May 8.html>

22. *May 07, Net4Nowt* — **BT Email: 41% Spam and 1 in 220 has Virus.** British ISP BT Openworld monitored mails sent by its customers between March 17, 2003 and March 23, 2003. **Of more than 25 million emails scanned, nearly 11 million were detected and trapped as spam.** This equates to a weekly average of 41 per cent. Thursday was the most popular day for spamming, with more than four million examples detected. Sunday polled the highest percentage of spam with the proportion rising to 51 percent of all messages sent. To make matters worse, **the filters also detected over 113,000 viruses – one for every 220 mails sent.**

Source: <http://www.ds-osac.org/view.cfm?KEY=7E44514A455C1E0A3A0F162820>

23. *May 07, National Journal* — **IT officials emphasize need for emergency backup systems. Many government offices must do better at backing up their information systems to preserve important data and ensure "continuity of operations" in the event of a terrorist attack,** several federal technology officials said on Tuesday at a homeland security conference sponsored by the Armed Forces Communications and Electronics Association. **FEMA's continuity-of-operations plan for many other systems typically amounts to "a pile of tapes" containing archived data,** said Robert Coxe, deputy CIO of the Federal Emergency Management Agency (FEMA). **Redundant communications and information systems**

proved invaluable after the attacks on the World Trade Center and the Pentagon, according to Lt. General Harry Raduege of the Defense Information Systems Agency. He recalled that **one military agency avoided major data losses during the Pentagon attack because its computer systems had "double backup" capabilities.** But he said officials in another Pentagon organization had stored "everything they had" on only one system that was destroyed in the attack. "They lost every bit of that data," he said.

Source: <http://www.govexec.com/dailyfed/0503/050703td2.htm>

Internet Alert Dashboard

Current Alert Levels	
 <p>AlertCon: 1 out of 4 https://gtoc.iss.net</p>	 <p>Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/</p>
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_LOVGATE.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	137 (netbios-ns), 6346 (gnutella-svc), 80 (www), 1434 (ms-sql-m), 445 (microsoft-ds), 113 (ident), 25 (smtp), 8627 (----), 139 (netbios-ssn), 9007 (----) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

24. *May 08, Associated Press* — **New tornadoes leave two dead in Illinois.** Residents across southern Illinois picked up what they could salvage from their wrecked homes and braced for more bad weather as tornadoes loomed in the forecast. **At least four tornadoes hit southern Illinois late Tuesday and early Wednesday, killing two people, injuring at least 20 and destroying or damaging scores of homes in three counties.** "It's a very, very rural area so the damage is very spread out," said Bill Burke, director of the Illinois Emergency Management Agency. Gov. Rod Blagojevich was considering declaring the region a state disaster area. Source: <http://www.washingtonpost.com/wp-dyn/articles/A28884-2003May 8.html>

25. *May 08, Sydney Morning Herald (Australia)* — **Al Qaeda preparing new September 11-type attack: report.** Al Qaeda is preparing a new attack in the United States on the scale of September 11 after adopting a new operational structure which is impenetrable to U.S. intelligence, a Saudi weekly reports in its Friday edition. "An attack against America is inevitable," Al-Majallah quotes the Islamic militant network's newly-appointed spokesman Thabet bin Qais as saying in an email to the paper. Al Qaeda has "carried out changes in its

leadership and sidelined the September 11, 2001 team," the paper quotes bin Qais as saying. **"Future missions have been entrusted to the new team, which is well protected against the U.S. intelligence services. The old leadership does not know the names of any of its members."**

Source: <http://www.smh.com.au/articles/2003/05/08/1052280363366.html>

26. *May 08, Associated Press* — **Saudis report arms seizure and foiling of terror attacks.** Saudi authorities have foiled plans by suspected terrorists to carry out attacks in the kingdom and have seized a large cache of weapons and explosives, the Interior Ministry said on Wednesday. **Security forces seized the weapons here in the capital on Tuesday as they were searching for suspects, an unidentified ministry official said. The official, quoted by the state-run Saudi Press Agency, said at least 19 men were being sought, including 17 Saudis, a Yemeni and an Iraqi holding both Kuwaiti and Canadian citizenship.** The official did not disclose what the men were targeting. Their names and pictures were shown on state-run Saudi television; the Interior Ministry official appealed to the public to help in apprehending them and warned against giving them shelter. **The weapons and explosives found in the damaged car and in an apartment where some of the men were staying included hand grenades, five suitcases of explosives weighing more than 830 pounds and AK-47 assault rifles, authorities said. Computers, communications equipment, travel documents, U.S. and Saudi currency and items used for disguise were also seized.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A28077-2003May 7.html>

27. *May 08, VOA News.com* — **U.S. completely rejects Iran's assertion of a peaceful nuclear program.** The United States said Thursday it "completely rejects" Iran's assertion that its nuclear program is for peaceful purposes only. **Bush administration officials say they will press for a finding by the International Atomic Energy Agency (IAEA), next month that Iran has violated the nuclear Non-Proliferation Treaty.** Officials here say concern is growing about the Iranian nuclear program, and that despite Tehran's assertions that the program is peaceful, **there is no doubt among U.S. experts that Iran has mounted an aggressive, and until recently covert, drive to acquire nuclear arms.** The full extent of the Iranian weapons effort began to come to light last August. An Iranian opposition group published satellite photos of what it said were two weapons-related nuclear sites under construction in central Iran, **one for enriching uranium and another for producing "heavy water," an essential ingredient for making plutonium.**

Source: <http://www.voanews.com/article.cfm?objectID=8AC94665-7CAF-4E4E-9FCF524BA22F5201>

28. *May 06, KCRA Channel.com* — **USDA event raises concern over violent protest.** Next month Sacramento will host an international gathering of agriculture ministers from more than 180 nations. It's an event that brings prestige and exposure to the city, but there is concern that some may try to use it as a platform for violence. **Police said a number of Web sites are sending out a "call to action" for a repeat of what happened in Seattle in 1999, when riotous protesters laid siege to the city during a World Trade Organization meeting. Sacramento police confirmed Tuesday that they are already working with the FBI, Department of Justice, and other federal and state authorities to stop any violent protests.** FBI officials said protest Web sites touting the event as a WTO meeting are misleading. In fact, it's a U.S. Department of Agriculture event meant to address agricultural issues. "Those letters are being

used to incite those who otherwise would not attend a conference like this," FBI spokesman Nick Rossi said.

Source: <http://www.thekrachannel.com/news/2185529/detail.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 202-324-1129

Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov 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.