



# National Infrastructure Protection Center NIPC Daily Open Source Report for 12 March 2003

Current Nationwide  
Threat Level is



[For info click here](#)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- The General Accounting Office has published report GAO-03-528T entitled "Emergency Preparedness Issues at the Indian Point 2 Nuclear Power Plant," in response to the increased concern over emergency preparedness at nuclear power plants. (See item [4](#))
- The Associated Press reports the United States government has announced it would help developing countries track down loose radioactive materials on their soil, the kind of step the chief UN nuclear watchdog said was "urgently needed" to foil terrorists bent on building "dirty bombs." (See item [21](#))
- CERT announces Advisory CA-2003-08: "Increased Activity Targeting Windows Shares," which has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. (See item [29](#))
- CNET News reports Internet Security Systems has announced that a serious security flaw has been found in business management software from PeopleSoft. (See item [31](#))

### NIPC 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](#); [NIPC 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. *March 11, Las Vegas Review - Journal* — **Nuclear waste: cask safety tests discussed . The Nuclear Regulatory Commission has began gathering comment on a plan to perform full-scale safety tests on nuclear waste shipping casks, with Nevada and other interests differing on how they should be conducted.** At the first public meeting on a new NRC

proposal, representatives from the state and public interest groups urged the agency to expand full-scale testing and make it an integral part of the agency's process for licensing cask designs. **Industry officials varied in their support while urging that the agency be cautious in considering the scope and cost of the experiments. Mark Holt, an observer and analyst for the Congressional Research Service, said the cask tests will be closely watched by federal lawmakers looking to shape future nuclear programs.** "The results of the study will be extremely important to future debates," he said. NRC staff has proposed high-speed collision tests that would drop a 25-ton truck cask and a rail cask weighing as much as 125 tons from a height that would simulate a 75 mph crash. Each cask then would be engulfed by a jet fuel fire for more than 30 minutes. The tests are the latest step in a package performance study the agency has been considering since 1999.

Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3701143](http://www.energycentral.com/sections/news/nw_article.cfm?id=3701143)

2. *March 11, The Washington Times* — **Al Qaeda plans oil field attacks** . Al Qaeda is seeking recruits in the Middle East for terrorist attacks on oil fields in Saudi Arabia and Kuwait in the event of U.S. military action against Iraq, U.S. intelligence officials say. **Meanwhile, U.S. officials said yesterday that there are signs that Iraqi leader Saddam Hussein's forces have planted explosives in Iraqi oil fields in anticipation of sabotaging them during U.S. and allied military attacks.** The al Qaeda recruitment is targeting radical Islamists in Saudi Arabia and Yemen who are willing to conduct suicide attacks and other sabotage against the oil fields outside Iraq. **The threats to oil facilities highlight the possibility that military action will disrupt the flow of oil from the Middle East, where most of the world's oil originates. Meanwhile, U.S. officials say they have detected signs recently that the Iraqis had planted explosives at oil facilities in Kirkuk, in northern Iraq.** "There are indications that has taken place," one official said. U.S. defense and intelligence officials said Iraqis have moved explosives toward oil fields in the south as well. The Pentagon released a statement last week that said U.S. forces would seek to prevent Iraqi sabotage of its approximately 2,000 oil wells, 500 in the northern part of the country and 1,500 in the south. **"Recent information revealed that Iraq has received 24 railroad boxcars full of pentolite explosives," the statement said. "U.S. plans are first to prevent the destruction of Iraq's oil fields and second, if unable to prevent the destruction, to control and mitigate the damage quickly."**

Source: [http://dynamic.washtimes.com/twt-print.cfm?ArticleID=2003031\\_1-535533](http://dynamic.washtimes.com/twt-print.cfm?ArticleID=2003031_1-535533)

3. *March 11, Associated Press* — **U.S. withholds approval for nuclear waste storage on Indian Reservation. Federal regulators today blocked a proposal by utility companies to store high-level nuclear waste on an Indian reservation in Utah's western desert, citing dangers posed by a nearby Air Force training range.** Private Fuel Storage, a consortium of eight electric utilities, had sought to store uranium rods from nuclear reactors in casks on the Skull Valley Goshute Reservation, 45 miles southwest of Salt Lake City, until a permanent storage complex could be built at Yucca Mountain in Nevada. Utah officials objected, raising a number of safety concerns, including the threat posed by military aircraft and earthquakes. The Air Force flies thousands of training missions a year over the sprawling Utah Test and Training Range, near the reservation. **"There is enough likelihood of an F-16 crash into the proposed facility that such an accident must be deemed credible," the Atomic Safety Licensing Board, an arm of the Nuclear Regulatory Commission, said in a 222-page opinion today.** As a result, the board said, it is withholding approval of the project. The board said it might reconsider its decision if Private Fuel Storage, or P.F.S., could either persuade the Air Force to

reduce the number of flights over the reservation or show that the concrete and steel casks where the waste would be stored could withstand an F-16 crash. **The proposed storage center would essentially be an 820-acre concrete parking lot. On it would be rows of 4,000 casks with concrete and steel walls, two and a half feet thick, encasing a total of 40,000 metric tons of uranium.**

Source: <http://www.nytimes.com/2003/03/11/politics/11UTAH.html>

- 4. *March 10, General Accounting Office* — GAO-03-528T: Nuclear Regulation: Emergency Preparedness Issues at the Indian Point 2 Nuclear Power Plant.** The General Accounting Office (GAO) has released GAO-03-528T: Emergency Preparedness Issues at the Indian Point 2 Nuclear Power Plant. **This was done in part because after the September 11, 2001 terrorist attacks, emergency preparedness at nuclear power plants has become of increased concern. Among other points, since the GAO's 2001 report, the Nuclear Regulatory Commission (NRC) has found that emergency preparedness weaknesses have continued.** For example, NRC reported that, during an emergency exercise in the fall of 2002, the facility gave out unclear information about the release of radioactive materials, which had also happened during the February 2000 event. **The GAO did not evaluate the draft Witt report or verify the accuracy of its findings.** GAO is aware that, in commenting on a draft of the Witt report, the Federal Emergency Management Agency disagreed with some of the issues and the NRC concluded it gave "undue weight" to the impact of a terrorist attack. Highlights: <http://www.gao.gov/highlights/d03528thigh.pdf>  
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-03-528T>

- 5. *March 09, The Daily Oklahoman* — Lawton-area Wind Farm to harvest power of Oklahoma's incessant gusts. Towering more than 300 feet above the Slick Hills northwest of Lawton, 38 giant windmills soon will produce enough electricity to meet the needs of 20,000 homes. The turbines will be turning by the end of this year and will comprise the state's first wind farm.** While people have been using wind as a source of energy for centuries, they have only recently figured out how to use it as a profitable way to generate electricity. Renewable energy advocates and western Oklahoma communities hail the Slick Hills project and hope the Blue Canyon Wind Farm project will be only the beginning of the wind power industry for Oklahoma. **"The economic development opportunities for the state are tremendous," said Tim Hughes, director of the Oklahoma Wind Power Initiative. "You get revenue for the landowners, new jobs and tax revenues for the counties and communities."** Wind has been harnessed for thousands of years and used for tasks ranging from tilling fields to powering naval fleets. **But wind has been used to generate commercial electricity for only about two decades.** Wind generators were relatively small when they became popular in the 1980s — 100 feet tall with a diameter of 40 feet and a maximum production of about 30 kilowatts. **The largest turbines in use today are more than 300 feet tall with a rotor diameter of more than 200 feet and can each produce between 1,500 and 3,000 kilowatts, enough to power up to 900 homes.** While wind energy technology continues to develop and the generators become more popular, it is unclear whether wind will ever rival the dominance fossil fuels hold on electrical generation.  
Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3700826](http://www.energycentral.com/sections/news/nw_article.cfm?id=3700826)

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

## Chemical Sector

Nothing to report.

[[Return to top](#)]

## Defense Industrial Base Sector

6. *March 11, Associated Press* — **Reserve call-up burden falling unevenly.** States like **Alabama, North Dakota and Nebraska have been hard hit by the mobilization of reserve and guard forces for the war on terrorism and a possible war with Iraq, leaving them short of prison guards, firefighters, policemen and even high school wrestling coaches. Other states, like Hawaii, New York and Michigan, have been asked to bear a much smaller share of the mobilization burden, according to an AP analysis of the Pentagon call-up and reserve force data.** Pentagon officials say the call-ups are based mostly on the needs of commanders in the field, and on the training, specialties and readiness of guard and reserve units back home. Impact on communities is considered but isn't a primary concern. "We don't measure contributions by numbers alone," said Lt. Col. Dan Stoneking, a Pentagon spokesman. "All 54 states and territories are supporting the war on terrorism. ... Each of those contributions is equally critical and equally appreciated." **The AP analysis found that North Dakota has shouldered the biggest burden, per capita, of any state. As of last week, 36 out of every 10,000 North Dakotans age 18 or older were serving on active duty from a reserve or National Guard unit. In New York, Michigan and Hawaii, though, fewer than five of every 10,000 eligible people were on active duty from a reserve or guard unit. In 19 other states, fewer than 10 of every 10,000 eligible people were under orders.**

Source: [http://www.washingtonpost.com/wp-dyn/articles/A8521-2003Mar1\\_1.html](http://www.washingtonpost.com/wp-dyn/articles/A8521-2003Mar1_1.html)

7. *March 11, Federal Computer Week* — **DISA releases bandwidth expansion RFP.** The Defense Information Systems Agency (DISA) last week issued a request for proposals (RFP) that will kick off the next phase of a project aimed at boosting the amount of high-speed bandwidth available to the military and intelligence communities. The Global Information Grid (GIG) bandwidth expansion is a cornerstone of the Defense Department chief information officer's vision for network-centric operations, in which data is posted on networks and made available departmentwide. **The RFP, issued March 7, includes specifications for equipment and fiber to bring the enhanced bandwidth to 92 approved locations worldwide. Contractors have until April 8 to reply, and awards are expected before the end of this fiscal year, according to DISA officials. DOD CIO John Stenbit anticipates providing a global, high-speed, low-latency optical IP network to military and intelligence bases worldwide, Army Col. Robert Horback, the GIG bandwidth expansion's program manager told FCW in an interview earlier this year.**

Source: <http://www.fcw.com/fcw/articles/2003/0310/web-disa-03-10-03.asp>

8. *March 10, Associated Press* — **Boeing lifts defense satellite into orbit.** After more than a month of delays, the Air Force launched a defense satellite Monday that will allow faster communication between U.S. defense officials and battlefield commanders. The blast off of the Boeing Delta 4 rocket was the first space launch in the United States since space shuttle Columbia broke up over Texas on Feb. 1. **The \$200 million satellite will become part of the**

**United States' national security communications network, which relays secure data to the White House, U.S. embassies and military personnel.** The launch was also the first military mission of an Air Force program designed to produce and launch rockets in a more efficient and less expensive manner.

Source: [http://www.washingtonpost.com/wp-dyn/articles/A8074-2003Mar1\\_0.html](http://www.washingtonpost.com/wp-dyn/articles/A8074-2003Mar1_0.html)

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

## **Banking and Finance Sector**

9. *March 11, Reuters* — **Terrorist fund flows likely to shift to Asia – FBI.** A crackdown on illegal money flows has forced Osama bin Laden's al Qaeda network to channel funds away from the Middle East, likely to Asia, a senior FBI officer said on Tuesday. **"They are looking for other routes they can transit their money through," said Dennis Lormel, the chief of the FBI's anti-terrorist financing unit, adding ... "it's a good possibility" that Asia could be an alternative.** The capture of alleged al Qaeda master planner Khalid Sheikh Mohammed this month, along with his computers, will provide leads for FBI agents seeking the money that has funded attacks such as the September 11 strikes and the Bali bombings, he said. **"Terrorists were moving money through the UAE (United Arab Emirates). They're shifting away from the UAE... It's more likely that you could see terrorists trying to penetrate this (Asian) market now," Lormel told a news conference during a visit in Hong Kong.**

Source: <http://www.alertnet.org/thenews/newsdesk/T161305>

10. *March 07, CNET News* — **E-mail scam tries to fool PayPal users.** PayPal subscribers are being targeted by a fraudulent e-mail scheme designed to con them into handing over their personal information. **Over the past week, users of eBay's online payments service have been receiving e-mails masquerading as official PayPal alerts, eBay spokesman Kevin Pursglove confirmed Friday. The messages ask recipients to submit bank and credit card details.** Tricks involving bogus e-mail posing as legitimate messages from eBay and PayPal are nothing new. However, the latest spoof e-mail—which included a PayPal logo, links to PayPal's site and official-looking fine-print—appeared particularly convincing, said Brenda Frymire, a PayPal user in San Ramon, CA, who received the e-mail Thursday. The e-mails tell recipients that their PayPal accounts have been randomly selected for maintenance and placed on "Limited Access" status. The message, which appears to come from info@paypal.com, instructs the account holder to enter credit card and bank account numbers in an online form embedded in the e-mail. **Pursglove said that the "spoof" e-mail did not come from eBay or its PayPal unit and that it is very likely a trick to rob people of private information. He said the company has received several complaints, but has yet to figure out who is behind the scheme. "We encourage people to notify us and not to respond to these e-mails," said Pursglove, noting that eBay makes it a practice not to request users' personal information via e-mail.**

Source: <http://news.com.com/2100-1018-991639.html>

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

## Transportation Sector

11. *March 11, Chicago Tribune* — **Anti-terror units eye missile peril to jets over city.**

Anti-terrorism agents are being sent to Chicago and airports in about 80 other cities to gauge the vulnerability of low-flying passenger planes to the threat of shoulder-fired missiles, FBI and Chicago officials said Monday. The need to safeguard aircraft goes well beyond the boundaries of O'Hare International Airport. **Protecting flights that approach and depart O'Hare and travel over forest preserves, lakes and remote but easily accessible locations—including cemeteries—is the main focus of the federal task force here. As part of their assessment, officials also will seek to tighten access to high-rise offices near O'Hare, including buildings along the Tri-State Tollway, to prevent the possibility of rooftop attacks.** Chicago officials, worried that aircraft could be targeted by portable heat-seeking missiles while flying over downtown, **have asked that Midway Airport and Meigs Field be included in the security review.**

Source: <http://www.chicagotribune.com/news/chi-0303110316mar11.1.333.8386.story>

12. *March 11, Washington Post* — **Is worst ahead for airlines? U.S. airlines, already in the weakest shape in memory because of terrorism, the economy and their own errors, are bracing for a fresh blow from a war in Iraq. The outbreak of hostilities is likely to drive up oil prices and keep legions of air travelers at home, intensifying the financial hardship of an industry already struggling under tons of red ink, massive layoffs and two major bankruptcies.** The airlines are preparing survival strategies that include prepaying for fuel to offset higher prices later, postponing delivery of aircraft, deferring employees' wages, renegotiating payments to suppliers and creditors and heavily lobbying Congress for relief. **The airlines are in a far more precarious condition than they were the last time the United States went to war in Iraq in 1991. The Sept. 11, 2001, terrorist attacks have crippled air travel, forced the elimination of many flights and raised the airlines' costs for security.** The weak economy and rising oil prices also have contributed to the carriers' steep losses. Air travel could drop 10 percent during a confrontation with Iraq, said the Air Transport Association, which plans to release a report today on the air industry crisis. **During the Gulf War, demand fell 8 percent -- at a time when travelers had fewer worries about terrorist attacks in the United States than they do today. Sept. 11 has erased that sense of security.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A7698-2003Mar1.0.html>

13. *March 10, Transportation Security Administration* — **Air travelers' security enhanced as**

**TSA intercepts over 4.8 million prohibited items in first year, including 1,101 firearms. The Transportation Security Administration has intercepted more than 4.8 million prohibited items at passenger security checkpoints in its first year, contributing to the security of the traveling public and the nation's 429 commercial airports. Through February, intercepted items included 1,101 firearms, nearly 1.4 million knives, nearly 2.4 million other sharp objects including scissors, 39,842 box cutters, 125,273 incendiary or flammable objects, and 15,666 clubs. "Those statistics are strong testimony to the professionalism and attention to detail of our highly trained security screeners," said Adm. James M. Loy, the TSA's administrator. "Although intercepting most of those items resulted from inadvertent violations by passengers, keeping dangerous items off flights is a top priority and we must err on the side of caution."**

Source: <http://www.tsa.gov/public/display?theme=44/font>

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

## **Postal and Shipping Sector**

14. *March 10, Chicago Tribune* — **U.S. works to shore up port security. As the U.S. shores up its borders and airports to avert another large-scale terrorist attack, experts increasingly are seeking a similar level of vigilance for the nation's 350 seaports.** Congress has allocated about \$500 million for security enhancements such as developing high-tech containers that can detect nuclear weapons as well as biological and chemical agents, and dispatching more security agents to inspect cargo at the point of origin. **Nevertheless, experts argue that billions of dollars are needed to plug the many gaps over the thousands of miles from the countries where goods are made to the retail shelves in the United States.** The security lapses and potential devastation to the economy were underscored last autumn when about 85 officials from the CIA, FBI, Office of Homeland Security and international trade businesses staged a war game centering on a terrorist plot to send weapons of mass destruction to the U.S. through the ports. In the scenario, authorities conducted a nationwide search of ports to thwart the attack. But days later, a "dirty bomb" that entered through an East Coast port in a shipping container exploded in downtown Chicago. **Participants concluded that ports are particularly vulnerable because they are equipped to inspect only about 3 percent of the 20,000 or so 24- and 48-foot-long containers that enter the U.S. every day. Moreover, those involved in the exercise determined that shutting down the port system would devastate commerce because more than 90 percent of imported goods arrive in the U.S. by sea.**

Source: <http://www.chicagotribune.com/news/nationworld/chi-0303100190mar10.1.1127794.story>

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

## **Agriculture Sector**

15. *March 11, Reuters* — **Dutch find suspected bird flu farm in new area.** Dutch authorities on Tuesday discovered the first farm suspected to be infected with bird flu outside the original contaminated zone. **So far the outbreak of bird flu, or avian virus, had been limited to a relatively small area in the central Gelderland province, but the new case was in the southern Zeeland province, Agriculture Ministry spokeswoman Martine de Haan told Reuters.** Exports have been banned from the Dutch poultry sector, which has around 100 million birds, since the outbreak was discovered last week in the world's fourth biggest poultry exporter and the largest in the European Union. It is an indication that the highly-infectious disease might have already spread into other areas of country, denting hopes of a quick end to the outbreak.

Source: <http://www.alertnet.org/thenews/newsdesk/L11249743>

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

## **Food Sector**

Nothing to report.

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

## Water Sector

Nothing to report.

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

## Public Health Sector

16. *March 11, Associated Press* — **San Diego firm to test anthrax vaccine. A San Diego biotechnology firm said Monday it hopes to begin human testing of its experimental anthrax vaccine by year's end.** Several companies and government researchers are racing to create a better anthrax vaccine than the one now available. **Company executives presented data Monday that showed their novel DNA vaccine protected rabbits that inhaled anthrax with little side effect, building upon their successful work with mice. Now the company hopes to convince the U.S. Food and Drug Administration (FDA) to allow it to test the two-injection regimen on a handful of people to prove the vaccine is safe.** The FDA said it will approve some vaccines that protect at least two different animal species and prove safe in human experiments.

Source: <http://www.bayarea.com/mld/cctimes/business/5364492.htm>

17. *March 11, Associated Press* — **West Nile may finish march across U.S. this year. West Nile virus may well complete its coast-to-coast spread this summer, infecting large numbers.** There's no good way to predict, as the deadly virus is from a family that's notoriously fickle. During last year's record-setting epidemic more than 4,000 people became ill and 274 died only a handful of states escaped human illness. But even some of those harbored infected mosquitoes and birds. Tackling this virus "is unbelievably complex," said. Lyle Petersen of the Centers for Disease Control and Prevention, the nation's chief West Nile specialist. **The one sure discovery is that "where West Nile has been, it stays." But Petersen said another large epidemic "would not be surprising," with West Nile hitting each of the 48 contiguous states.** Not counting Alaska and Hawaii, only nine states have escaped human illness so far. Of particular concern is the West, where the virus was just encroaching when winter hit. Only four states – Oregon, Nevada, Utah and Arizona – appear free of the virus, which first appeared in New York in 1999.

Source: [http://rockymountainnews.com/drmn/state/article/0,1299,DRMN\\_21\\_1802714,00.html](http://rockymountainnews.com/drmn/state/article/0,1299,DRMN_21_1802714,00.html)

18. *March 11, Health-News.co* — **New technique in fight against bioterrorism.** A UK researcher has developed a new technique to speed up detection of infections that could prove devastating if used as a biological weapon by terrorist groups. **Dr Colm Lowery, from the School of Biological and Environmental Sciences at the University of Ulster, has pioneered a new DNA fingerprinting technique that takes only minutes to identify potentially deadly bacteria. Tests usually take up to five days to identify killer bugs such as E. coli and Cryptosporidium, which terrorists could use to contaminate water supplies. However, the new test only takes 15 minutes and could therefore save thousands of lives in the event of a biological attack.** Dr Lowery said, "Because the DNA fingerprinting technology is so fast it

will be invaluable in the event of a biological attack, allowing the quick detection of the source and type of agent that has been used. "Subsequently, it will be easier to treat victims and prevent more outbreaks. The bottom line is that the introduction of these new technologies will help save lives." **The new DNA fingerprinting techniques can also be applied to the routine monitoring of food and water quality, as well as other areas of medical research.**

Source: <http://www.health-news.co.uk/showstory.asp?id=108157>

19. *March 11, Reuters* — **FDA warns of bacteria-laced fake anemia drug. U.S. regulators warned health officials and consumers on Tuesday to be on the lookout for bacteria-tainted fakes of a popular anemia drug.** Investigators at the U.S. Food and Drug Administration (FDA) said three lots of Procrit, an anemia drug aimed at coaxing production of red blood cells, were tainted with bacteria that make the product a "significant potential hazard to consumers." **Regulators say production of phony medicines is rising, as counterfeiters become more sophisticated and Americans seek low cost drugs.**

Source: <http://reuters.com/newsArticle.jhtml?type=scienceNewsD=2361787>

20. *March 10, American Society for Microbiology* — **Combination therapy improves anthrax survival. Treating anthrax patients with a combination of antibiotics and antibodies could greatly improve their likelihood of survival, say researchers today at the American Society for Microbiology's Biodefense Research Meeting.** "Currently there is no effective treatment for inhalation anthrax beyond administration of antibiotics shortly after exposure," says Vladimir Karginov a lead researcher in the study. "Time delay reduces the effectiveness of antibiotic treatment. There is need for new, safe and effective treatments to supplement traditional antibiotic therapy." **Antibiotic therapy for inhalation anthrax is generally only effective if it is started within days of exposure, before symptoms appear. By the time symptoms do appear antibiotics alone will not work because anthrax toxin has already accumulated in the body to dangerous levels and the chances of dying are extremely high. Karginov and his colleagues have developed a treatment strategy that addresses this problem. In addition to antibiotics to kill the infection, patients can also be given antibodies that programmed to attack a part of the toxin called the protective antigen and prevent it from doing damage.**

Source: [http://www.eurekalert.org/pub\\_releases/2003-03/asfm-cti03070\\_3.php](http://www.eurekalert.org/pub_releases/2003-03/asfm-cti03070_3.php)

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

## **Government Sector**

21. *March 11, Associated Press* — **U.S. to boost aid against 'dirty bombs'.** The United States announced Tuesday it would help developing countries track down loose radioactive materials on their soil, the kind of step the chief UN nuclear watchdog said was "urgently needed" to foil terrorists bent on building "dirty bombs." **The U.S. energy secretary, Spencer Abraham, said Washington would spend \$3 million in the next year to help poorer governments secure high-risk radiation sources that could be used for terror weapons. "The threat requires a determined and comprehensive international response," Abraham told the opening session of the first high-level global conference on what are technically known as radiological dispersal devices. The U.S. and Russian governments joined forces as co-sponsors to bring together hundreds of scientists and government officials for the**

**three-day gathering, to confront a threat that hasn't materialized yet but that could plunge cities into chaos if it does.** A recent California's Monterey Institute of International Studies' report concludes that worldwide "several tens of thousands" of the most dangerous radiation sources – used to treat cancer, find oil deposits, disinfect food – may be insufficiently protected. The MIIS study is available at <http://cns.miis.edu/pubs/opapers/op11/index.htm> In Washington, Sen. Hillary Rodham Clinton, D–NY, and Rep. Edward Markey, D–MA, have introduced legislation to establish a nationwide system of tracking radiation sources. Source: [http://story.news.yahoo.com/news?tmpl=story2611/ap\\_on\\_re\\_eu/dirty\\_bombs](http://story.news.yahoo.com/news?tmpl=story2611/ap_on_re_eu/dirty_bombs)

22. *March 11, Department of Justice, Office of the Inspector General* — **Audit No. 03–15: The Immigration and Naturalization Service's Primary Inspections at Air Ports of Entry.** The Department of Justice Audit No. 03–15 evaluates the Immigration and Naturalization Service's (INS) procedures for referring persons to secondary inspection, including critical associated functions relating to analyses of advance passenger information, availability of needed law enforcement information, and inspector training. The report contains recommendations for specific and immediate steps the INS should take to improve its primary inspection operations at air ports of entry (POEs). Such analyses are critical in identifying high–risk individuals so that primary inspectors can prevent the entry of inadmissible persons into the United States. The INS also needs to strengthen its policy, controls, and mechanisms to ensure that vital lookout and sensitive intelligence information is available to primary inspectors. Additionally, the INS needs to strengthen controls over the entire primary inspection process. **Further, the INS needs to ensure that the training provided to new inspectors is sufficient to enable them to use the computer systems that provide lookout and other critical information on travelers seeking entry into the United States.** The fact that in FY 2002 approximately 26 percent of all inspectors at air, land, and sea POEs were newly hired only increases the need for the INS to implement an aggressive and complete inspector training program. Source: <http://www.justice.gov/oig/audit/0315/exec.htm>

23. *March 11, The White House* — **Director of Terrorist Threat Integration Center announced.** On March 11th, John O. Brennan was named the Director of the newly created Terrorist Threat Integration Center (TTIC). The TTIC, which was announced by the President in his State of the Union Address, is scheduled to begin operations on May 1, 2003. It will enable full integration of U.S. Government terrorist threat–related information and analysis. Its structure is designed to ensure rapid and unfettered sharing of relevant information across department lines. **Brennan was appointed by the Director of the Central Intelligence Agency, George J. Tenet, in consultation with the Director of the FBI, the Attorney General, and the Secretaries of Homeland Security and Defense.** Source: <http://www.whitehouse.gov/news/releases/2003/03/20030311.htm>

24. *March 11, Government Executive* — **Congress probing links between immigration, terrorism.** As Congress begins grappling with the question of how to tighten border security, lawmakers have introduced more than 90 immigration–related bills so far—many focusing on homeland security concerns. At issue: Can the nation tighten security while protecting the rights of legal immigrants? House Judiciary Committee Chairman James Sensenbrenner, R–WI, and ranking member John Conyers, D–MI, have urged Homeland Security Secretary Tom Ridge to focus on immigration issues. **The proposed legislation covers a range of issues—from trying to restrict immigration to providing more manpower at the border.**

Rep. Sheila Jackson Lee, D–TX, is sponsoring several measures, including one calling for a study of traffic stops along the border. Conyers has introduced a bill amending the Immigration and Nationality Act to guarantee due process in immigration proceedings and require reports from the attorney general on those detained after September 11, 2001.

Source: <http://www.govexec.com/dailyfed/0303/031003cd1.htm>

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

## Emergency Services Sector

25. *March 11, Associated Press* — **Ridge announces anti–terror city funding.** Homeland Security Director Tom Ridge announced **\$750 million in grants Monday to help rural, urban and suburban fire departments better train, prepare and equip for the war on terrorism.** Ridge urged about 3,000 mayors and council members attending this year's National League of Cities legislative conference to use the Assistance to Firefighters grants wisely. **He recommended that leaders pool their resources in mutual aid agreements between neighboring cities, or to develop new training programs and buy equipment.** Ridge's announcement more than doubled last year's Assistance to Firefighters grants, when the Federal Emergency Management Agency distributed more than \$334 million through 5,316 grants to help America's firefighters prepare to respond to fires and other disasters. FEMA is part of the Homeland Security Department.

Source: [http://www.washingtonpost.com/wp-dyn/articles/A7515-2003Mar1\\_0.html](http://www.washingtonpost.com/wp-dyn/articles/A7515-2003Mar1_0.html)

26. *March 11, Statesman Journal* — **State prepared for emergencies.** Governor Ted Kulongoski of Oregon said Monday that state agencies are prepared to respond to emergencies if a war in the Middle East triggers acts of terrorism comparable to those on the East Coast on Sept. 11, 2001. "There are no specific threats to the state of Oregon, but I believe it is wise to be prepared in the event of a disaster," Kulongoski said after a discussion with the Governor's Security Council. **Kulongoski spoke at the newly opened Emergency Operations Center on State Street, where the Oregon National Guard, Oregon State Police, Oregon Emergency Management and other agencies would respond to disasters, either natural or human–caused.**

Source: <http://news.statesmanjournal.com/article.cfm?i=58118>

27. *March 10, Federal Computer Week* — **Nebraska city sounds PC alarms.** Lincoln, NE, soon will implement a PC–based service that would instantly alert residents of the city and Lancaster County about severe local weather conditions, state notifications of abducted children and national homeland security warnings. Within a week the public would be able to download the program from the city Web site, said Terry Lowe, systems project manager with the city's Information Services Division. Once downloaded, the program will appear as an icon on a user's desktop or task manager. **When an alert is sent, a noise – like the loud "whooping" alarm heard on TV or radio when the Emergency Alert System is activated – would sound on a user's computer. That alarm would be followed by a pop–up screen explaining the type of emergency. Users would then be directed to other Web sites for additional information.** In the future, Lowe said **the alert will be available on personal digital assistants, wireless phones and beepers.**

Source: <http://www.fcw.com/geb/articles/2003/0310/web-lincoln-03-10-03.asp>

28. *March 10, Associated Press* — **Emergency teams shift focus to terrorism at Nevada conference.** Emergency workers who before Sept. 11 focused on floods, earthquakes and other natural disasters now find themselves on the front line against terrorism. **More than 2,000 firefighters, health care workers, military personnel and others attending a national conference that began Monday are learning how to prepare for the worst.** "We are here at a pivotal moment" when the country faces the threat of war and terrorism, said Dr. Robert Claypool, director of readiness and emergency response for the Veteran Affairs Department. "Yet we have every confidence they (emergency responders) will rise to the challenge. This group of people represents the best of America," he said. **The emergency workers are attending the annual meeting of the National Disaster Medical System, a federally coordinated program for responding to medical emergencies.**

Source: <http://www.lasvegassun.com/sunbin/stories/nevada/2003/mar/10/031010889.html>

[[Return to top](#)]

## **Information and Telecommunications Sector**

29. *March 11, CERT/CC* — **CERT Advisory CA-2003-08: Increased Activity Targeting Windows Shares.** Over the past few weeks, the CERT/CC has received an increasing number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. The presence of any of these tools on a system indicates that the Administrator password has likely been compromised, and the entire system is therefore suspect. With this level of access, intruders may exercise remote control expose confidential data; install other malicious software; change files; delete files; or launch attacks against other sites. **Information on how to guard against these attacks may be found on the CERT/CC website.**

Source: <http://www.cert.org/advisories/CA-2003-08.html>

30. *March 10, eWEEK* — **Federal government moves to secure net.** The White House and the new Department of Homeland Security have begun in earnest the process of implementing the plan to secure the nation's critical networks. The most significant move is the development of a private, compartmentalized network that will be used by federal agencies and private-sector experts to share information during large-scale security events, government officials said at the National Information Assurance Leadership conference in Washington D.C. last week. **The system is part of the newly created Cyber Warning Information Network (CWIN), a group of organizations including the National Infrastructure Protection Center, the Critical Infrastructure Assurance Office and others that have some responsibility for the security of federal systems. The private-sector Information Sharing and Analysis Centers will also be included. The CWIN, a key part of the Bush administration's National Strategy to Secure Cyberspace, will use a secure, private IP network separate from the public Internet,** according to officials. As part of the plan to improve security, the CIO of each federal agency is, by statute, now accountable for the security of that agency's

network.

Source: <http://www.eweek.com/article2/0,3959,922570,00.asp>

**31. March 10, CNET News — Security alert posted for PeopleSoft.** A serious security flaw has been found in business management software from PeopleSoft. **The flaw, known as a remote command execution vulnerability, gives outsiders the ability to install malicious computer code on PeopleSoft customers' Web servers, potentially leading to a "complete compromise" of their PeopleSoft business systems,** according to Internet Security Systems (ISS), the Atlanta-based computer security company that issued the warning on Monday. PeopleSoft supplies software designed to streamline accounting, human resources, sales and manufacturing activities to more than 5,000 companies around the world. **The flaw affects only certain releases of PeopleSoft version 8,** which the company began shipping in 2000. **Nearly 2,000 companies have installed version 8,** according to PeopleSoft spokesman Steve Swasey. **The patches and details about the vulnerability are available on the company's private Web site for PeopleSoft customers: [www.peoplesoft.com](http://www.peoplesoft.com).** PeopleSoft has yet to hear of any problems related to the security flaw, Swasey added.

Source: [http://news.com.com/2100-1009-991907.html?tag=fd\\_top](http://news.com.com/2100-1009-991907.html?tag=fd_top)

### Internet Alert Dashboard

Current Alert Levels	
 <p>AlertCon: 1 out of 4 <a href="https://gtoc.iss.net">https://gtoc.iss.net</a></p>	 <p>Security Focus ThreatCon: 1 out of 4 <a href="http://analyzer.securityfocus.com/">http://analyzer.securityfocus.com/</a></p>
Current Virus and Port Attacks	
<b>Virus:</b>	#1 Virus in the United States: <b>WORM_KLEZ.H</b> Source: <a href="http://wtc.trendmicro.com/wtc/wmap.html">http://wtc.trendmicro.com/wtc/wmap.html</a> , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
<b>Top 10 Target Ports</b>	137 (netbios-ns), 80 (www), 1434 (ms-sql-m), 445 (microsoft-ds), 113 (ident), 6346 (gnutella-svc), 139 (netbios-ssn), 4662 (eDonkey2000), 25 (smtp), 53 (domain) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center

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

## General Sector

**32. March 11, New York Times — Germans convict four Algerians in plot to bomb a French market.** A German court today convicted four Algerian men of plotting to blow up a crowded street market in Strasbourg, France, more than two years ago, sentencing them

**to 10 to 12 years in prison. The court said the men conspired to plant a bomb on New Year's Eve, when the cobbled streets of Strasbourg's old quarter would have been thronged by revelers.** The verdict came three weeks after a court in Hamburg convicted Mounir el-Motassadeq of 3,066 counts of murder for his role in the attack that leveled the World Trade Center. **Judge Zeiher noted that the men were not followers of Osama bin Laden, and did not have contact with those who plotted the Sept. 11, 2001, attacks while living in Hamburg.** Still, there were eerie parallels: These men are believed to have trained at terrorist camps in Afghanistan. They hatched their plot in apartments in Frankfurt, blending into the city's polyglot community. They traveled regularly in and out of Germany as the planning took shape. **The defendants – Aeurobui Beandali, Lamine Maroni, Salim Boukari, and Fouhad Sabour – were subdued during the two-hour reading of the verdict, stealing occasional glances at one another. Only Beandali spoke, saying he would not appeal the judgment.**

Source: <http://www.nytimes.com/2003/03/11/international/europe/11GER M.html>

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

## NIPC Products & Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC 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 NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following NIPC products:

[NIPC Warnings](#) – NIPC Assessments, Advisories, and Alerts: The NIPC produces three levels of infrastructure warnings which are developed and distributed consistent with the FBI's National Threat Warning System. 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.

[NIPC Publications](#) – NIPC Daily Reports, CyberNotes, Information Bulletins, and other publications

[NIPC Daily Reports Archive](#) – Access past NIPC Daily Reports

### **NIPC Daily Open Source Report Contact Information**

Content and Suggestions: [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the NIPC Daily Report Team at 202-324-1129

Distribution Information Send mail to [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) for more information.

### **Contact NIPC**

To report any incidents or to request information from NIPC, contact the NIPC Watch at [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov) or call 202-323-3204.

### **NIPC Disclaimer**

The NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal NIPC tool intended to

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