



# National Infrastructure Protection Center

## NIPC Daily Open Source Report for 24 February 2003

Current Nationwide Threat Level is



[For info click here](#)

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

### Daily Overview

- The Associated Press reports a cloud of ammonia leaked from a Mississippi chemical plant early Sunday, forcing hundreds of tourists to evacuate several hotels along the Gulf Coast. (See item [9](#))
- The Department of the Treasury and the Financial Crimes Enforcement Network have issued additional USA PATRIOT Act regulations, concerning a requirement that additional categories of financial institutions establish an anti-money laundering program. (See item [14](#))
- CERT has released Advisory CA-2003-06: Multiple vulnerabilities in implementations of the Session Initiation Protocol, which may allow an attacker to gain unauthorized privileged access, cause denial-of-service attacks, or cause unstable system behavior. (See item [28](#))
- Wired reports America Online says hackers gained full access to its customer database application last week, potentially exposing the personal information of AOL's 35 million users. (See item [29](#))

### 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: High, Cyber: High**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - <http://esisac.com>]

1. *February 23, Staten Island Advance* — **Could the Island blow up?** Staten Island is surrounded by potential toxic and explosive disasters. Millions of gallons of explosive fuel flows in pipes under ground and on ships along the coast. Each day, enormous tankers and barges deliver millions of gallons of flammable gasoline, oil and petroleum products to nearly 20 storage

facilities lining the New Jersey shoreline just across the Kill van Kull and Arthur Kill as well as one on Staten Island. **The dangers of having such volatile materials so close became grimly apparent Friday when a barge explosion at the Island's prime petroleum storage facility at Port Mobil in Charleston killed two workers, seriously injured another and sent plumes of thick, black smoke across the borough.** The barge was unloading 100,000 barrels of unleaded gasoline at the time. Authorities quickly ruled out a terrorist attack, but said the accident is under investigation. They are focusing on a barge pump that had been repaired only hours before the blast. Although the damage was relatively minimal, some officials said the explosion could have touched off a catastrophic chain reaction had it ignited nearby storage tanks. There are 39 tanks with a total capacity of 2.9 million barrels of gasoline and heating oil in the 203-acre site off Ellis and Arthur Kill roads. It is operated by ExxonMobil, the world's largest oil company. **In addition, officials worried the blast could have ruptured one of the massive pipelines beneath the ground. The Colonial Pipeline, which runs to the Northeast from Gulf Coast oil refineries, ends at Port Mobil. Others, including the Buckeye and Transcontinental pipelines, enter the borough elsewhere on the West Shore and pass through, supplying jet fuel to Kennedy and LaGuardia airports in Queens. While the waters are being watched, there's some concern landside about the spider web of pipes carrying natural gas and fuel across the borough. The two major pipelines are operated by Transcontinental Corp. and Buckeye Pipeline Co.**

Source: [http://www.silive.com/news/advance/index.ssf?/base/news/1046\\_009813213030.xml](http://www.silive.com/news/advance/index.ssf?/base/news/1046_009813213030.xml)

2. *February 23, New York Times* — **FEMA Study falls short, Indian Point opponents say.** Proponents of closing the Indian Point power plant claimed a modest victory yesterday with the Federal Emergency Management Agency's decision to withhold its endorsement of emergency plans at the nuclear plant. In virtually the same breath, however, the critics of contingency plans at the nuclear reactor said that FEMA did not go far enough when it reported on Friday that it could not offer "reasonable assurance" that evacuation routes or other measures would prove effective in the event of an accident or terrorist attack. **In its 500-page preliminary report, FEMA said that its uncertainty over emergency preparedness in the communities surrounding the plant — in Buchanan, Westchester County, about 35 miles north of Manhattan — stemmed from the state's failure to provide detailed information about what specific steps those communities would take if a catastrophe were to occur. It is unclear what action the Nuclear Regulatory Commission might take without state or FEMA certification of the emergency plan, which includes such details as evacuation procedures within 10 miles of the plant.** The commission has never denied a license based on uncertified emergency planning procedures, and it would likely ask that the state address any deficiencies with the contingency measures before making a decision about the plant's continued operation. That process could take months and would likely face a raft of legal challenges from both sides.

Source: [http://www.nytimes.com/2003/02/23/nyregion/23INDI.html?ntem\\_ail0](http://www.nytimes.com/2003/02/23/nyregion/23INDI.html?ntem_ail0)

3. *February 21, Reuters* — **Colonial Pipe into Staten Island diverted after blast. Oil products duct Colonial Pipeline Co. said on Friday the explosion of a gasoline barge off Staten Island forced it to shut down its line delivering oil products into the island, but it successfully diverted oil products to other terminals. Colonial, which runs from Houston to New York, is the largest U.S. oil products pipeline.** Susan Castiglione, a Colonial spokeswoman, said it shut a small line from Colonial to Staten Island out of "conservative

precautionary measures." She declined to tell the capacity of the line, citing company policy after the September 11, 2001 attacks on New York and Washington, D.C. A consortium jointly-owned by 10 oil companies, Colonial pumps a total of 2.35 million barrels-per-day (bpd) of gasoline and distillates.

Source: [http://biz.yahoo.com/rm/030221/energy\\_colonial\\_diversion\\_1.h tml](http://biz.yahoo.com/rm/030221/energy_colonial_diversion_1.h tml)

4. *February 20, Reuters* — **States threaten to sue U.S. government on pollution.** Seven states threatened on Thursday to sue the U.S. government to force a crackdown on carbon dioxide emissions from power plants, a response to the Bush administration's policy of asking companies to voluntarily control pollution. **Attorneys general from New York, Connecticut, Maine, Massachusetts, New Jersey, Rhode Island and Washington said the Environmental Protection Agency should update its list of pollutants to include carbon dioxide because the so-called greenhouse gas traps heat in the atmosphere and contributes to global warming.** Led by New York Attorney General Eliot Spitzer, a Democrat, the states said they were forced to act after the Republican Bush administration, rather than instituting mandatory controls, gathered agreements in recent months from utilities, automakers and oil refiners to voluntarily curb emissions of carbon dioxide and other greenhouse gases. **The current criteria pollutants, designated as hazardous to human health and subject to EPA standards, are carbon monoxide, lead, nitrogen oxides, ozone, particulate matter and sulfur oxides.**  
Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3660099](http://www.energycentral.com/sections/news/nw_article.cfm?id=3660099)
  
5. *February 20, Reuters* — **FERC approves some Midwest transmission grid transfers. The Federal Energy Regulatory Commission (FERC) wants to stitch together the nation's patchwork transmission grid to reduce bottlenecks and costs for consumers.** That effort is moving the fastest in the Midwest under a transmission grid-sharing arrangement called the Midwest Independent Transmission System Operator (ISO). Federal regulators on Thursday approved a transfer of some DTE Energy Co. transmission assets to create a new kind of independent grid company, but delayed a similar plan involving Dynegy Inc. assets because it may boost power rates. **The FERC said it would allow DTE Energy to transfer control of its transmission grid to subsidiary International Transmission Co. (ITC), which will operate the grid independent of the utility's control.** The company would operate on a new business model and derive its profits exclusively from moving other companies' power across its grid. Traditionally, utilities have controlled both the generation and transmission of power, but the agency is seeking to separate those two functions to cut down on what it sees as discriminatory practices.  
Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3660113](http://www.energycentral.com/sections/news/nw_article.cfm?id=3660113)
  
6. *February 20, Greenwire* — **New York regulators clear new distributed generation incentives.** The New York Public Service Commission on Wednesday ordered the state's major natural gas utilities to file special delivery rates for nonresidential customers who operate their own gas-fired distributed generation (DG) units, a move that should result in lower costs for DG operators and provide incentives for more widespread use. **Unlike large gas-fired power plants, DG units — often driven by fuel cells and microturbines — can be located off the overburdened grid and distributed throughout a utility's service territory, thus easing congestion. But because the technology is so new and traditional utilities are so entrenched behind restrictive interconnection standards, existing gas delivery rates for DG operators are higher than they should be, the PSC explained, justifying action to**

**make delivery more economical.** The American Gas Association's director of media relations, Peggy Laramie, explained that with the incentives, supermarkets, schools and small businesses might be more willing to consider installing cogeneration technologies, like a combined heat and power microturbine system that burns gas to produce power and recycles steam for other uses. **An example of where the technology is thriving is the 48-story Time-Life Building in Manhattan's Rockefeller Center, where the building's owners have reduced energy costs by one-third since switching last spring to a new central hybrid chiller plant that uses natural gas, electricity and steam. Having all three fuel sources gives the building's energy manager the option of picking the least expensive fuel at any given time.**

Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3660228](http://www.energycentral.com/sections/news/nw_article.cfm?id=3660228)

7. *February 20, Tulsa World* — **Oklahoma-based utility to offer wind-generated electricity.** Recognizing a significant growth in wind power projects and a demand for renewable energy, OG&E Electric Services announced plans Wednesday to provide wind-generated electricity to its customers. **The utility requested bids on 50 megawatts of wind power. The request, which was made specifically for OG&E's retail customers, is one of the largest of its kind, OG&E said. OG&E customers could begin receiving wind power by the fall of next year under the utility's plan.** However, customers who select the wind power option will be paying slightly more for the electricity because the cost to produce it is higher than production costs for coal- or gas-fired electricity, OG&E said. OG&E is the state's largest electric utility, serving 700,000 customers. Some customers will be willing to pay the higher prices because of the environmental benefits of wind farms. Unlike coal- and gas-fired power plants, wind farms don't pollute the air or water. **Texas and Kansas have experienced a boom in wind farm construction. In Texas, about 1,000 megawatts of wind power generation was built in 2001.** Based on today's gas prices, wind power is cheaper than gas-fired power, said Charles Ward, a member of the Oklahoma Renewable Energy Foundation. New technologies have helped lower the cost of wind power enough to compete with coal- and gas-fired power, Ward said.

Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3659997](http://www.energycentral.com/sections/news/nw_article.cfm?id=3659997)

8. *February 20, CNN* — **FBI investigates oil plant assault . The FBI is investigating a possible terror-related incident in southeastern Utah in which a man at an oil processing plant reported being assaulted by two Middle Eastern men who questioned him about the plant's operations, authorities said Thursday.** Kevin Eaton, a supervisory FBI special agent in Salt Lake City, said they received a report "that is terrorism-related and we're responding to it." He said an individual said he "was confronted by Middle Eastern men and questions were asked." **The alleged incident occurred around 11:30 p.m. Wednesday at an oil processing plant owned by Exxon-Mobil on a Navajo land near the small town of Aneth in the remote southeastern corner of the state, said Rick Bailey, the director of San Juan County Emergency Management.** The man reported that the two left in a dark-colored GMC Yukon, with four doors and dark-tinted windows. The vehicle did not have a front license plate and it was unclear if a tag was on the back, said Bailey.

Source: <http://www.cnn.com/2003/US/West/02/20/utah.terror.probe/index.html>

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

## **Chemical Sector**

9. *February 23, Associated Press* — **Ammonia leak forces Mississippi evacuation.** A cloud of ammonia leaked from a chemical plant early Sunday, forcing hundreds of tourists to evacuate several hotels along the Gulf Coast. Authorities said it appeared someone had tried to steal the chemical, possibly to make illegal drugs. **Police Sgt. Joseph Ashmore said investigators had found evidence that someone who apparently planned to use anhydrous ammonia to make crystal methamphetamine had tampered with a 2,000-gallon tank at the Channel Chemical plant in the Gulfport Industrial Seaway. About 600 gallons was missing, though investigators didn't know how much of that had leaked.** Gulfport-Biloxi International Airport was also shut down for seven hours, and several churches canceled or postponed Sunday services after police advised residents to stay indoors. The evacuation from about 2:30 a.m. to 9:30 a.m. affected six or seven hotels near the Gulf of Mexico shore, as well as an all-night Wal-Mart and several small restaurants. Officials also closed a 10-mile stretch of Interstate 10 and a 3-mile section of U.S. 49 and surrounding streets after a policeman spotted the chemical cloud. **Anhydrous ammonia, used to make fertilizer, is highly explosive. Exposure irritates the skin and airways and can be fatal.**

Source: <http://www.guardian.co.uk/uslatest/story/0,1282,-2427474,00.html>

10. *February 22, Courier-Journal (Louisville, KY)* — **Tests find air safe; search for cause starts. With the fire, last Thursday, at the CTA Acoustics plant (Corbin, KY), extinguished and environmental concerns eased, dozens of state and federal investigators yesterday began what they said could be a lengthy probe.** "This could take weeks before we know what happened, or why," said Brian Reams, incident commander coordinating the response to Thursday's explosion and fire at the plant. Agents from the federal Bureau of Alcohol, Tobacco and Firearms began touring the extensively damaged plant yesterday morning, and expect to remain on site until at least tomorrow. Members of the federal Chemical Safety and Hazard Investigation Board also are investigating what, if anything, could have prevented the explosion that injured 44 people and left at least 14 with extensive burns. **State and federal environmental officials said continued testing of air in and around the plant, as well as downstream water samples, revealed marginal amounts of toxins, but not enough to endanger the environment or neighbors.** CTA Acoustics officials were allowed to tour the site yesterday afternoon and will be permitted to use shipping docks and some offices once Occupational Safety and Health Administration officials determine the building is safe.

Source: [http://www.courier-journal.com/localnews/2003/02/22/ke022203\\_s370499.htm](http://www.courier-journal.com/localnews/2003/02/22/ke022203_s370499.htm)

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

## **Defense Industrial Base Sector**

11. *February 21, Washington Post* — **Pentagon buys escape masks for local use.** The Defense Department has purchased 80,000 "escape masks" to protect employees and visitors against chemical and biological attacks and will begin distributing them next week at the Pentagon and 46 other leased buildings in the area, defense officials announced yesterday. **Lt. Cmdr. Jeff Davis, a Pentagon spokesman, said the Survivair Quick 2000 masks, which cost \$150 apiece, would enable employees, contractors and visitors to safely make their way out of a building or area that has been attacked with poisonous chemicals or biological toxins. The masks, which come packed in a vacuum bag, would not be reusable. Davis said everyone**

working at the Pentagon and leased buildings would receive training when they are issued a mask, which they will have to sign for. The Defense Department will distribute about 500 masks a day, starting next week, he said. Caches of masks will be stored throughout the Pentagon for use by visitors.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A38196-2003Feb 20.html>

12. *February 21, Washington Post* — **U.S. bolsters Philippine force.** The United States is sending about 3,000 troops to engage in a major combat offensive in the southern Philippines aimed at wiping out the militant Muslim group Abu Sayyaf, Pentagon officials said yesterday. **The move marks the second time in less than a year that the Bush administration has committed a significant number of U.S. forces to try to root out the extremist group, which has continued to unsettle the Philippines and target Americans in the islands. It opens another battlefield as U.S. forces already are stretched thin preparing for a possible war in Iraq, securing Afghanistan and pursuing al Qaeda around the world.** Last year, nearly 1,300 U.S. advisers and support personnel participated in what was billed as a six-month training mission to bolster the counterterrorism capabilities of Philippine forces. That effort, which focused on the island of Basilan and concluded as scheduled on July 31, was credited with killing or capturing some Abu Sayyaf members, but it also ended up scattering scores of rebels to other islands. **This time, Pentagon officials are describing the mission not as a training exercise but a combat operation with no pre-set termination date. Although Philippine forces will have the lead, they will be accompanied in the field by American troops that will remain under U.S. command and be at some risk, defense officials said.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A37451-2003Feb 20.html>

13. *February 20, Associated Press* — **West Point beefs up anti-terror training.** The U.S. Military Academy opened an anti-terrorism center Thursday aimed at giving cadets more instruction on the topic. **Retired Army Gen. Wayne Downing will be chairman of the new Combating Terrorism Center, which will have a staff of four and will try to add more on bioterrorism, cyber-terrorism and other such topics to the curriculum.** The anti-terrorism curriculum at West Point now consists of just one elective.

Source: [http://story.news.yahoo.com/news?tmpl=story\\_p\\_on\\_re\\_us/west\\_point\\_terror\\_2](http://story.news.yahoo.com/news?tmpl=story_p_on_re_us/west_point_terror_2)

[[Return to top](#)]

## **Banking and Finance Sector**

14. *February 21, Department of the Treasury* — **Treasury Department issues additional USA PATRIOT Act regulations.** The Department of the Treasury and the Financial Crimes Enforcement Network (FinCEN) on Friday issued a proposed rule and two advance notices of proposed rulemaking concerning a requirement that additional categories of financial institutions establish an anti-money laundering program. **In a proposed rule, Treasury and FinCEN propose to require certain dealers in precious metals, precious stones, and jewels to establish an anti-money laundering program designed to detect and prevent money laundering and the financing of terrorism.** The proposed rule covers a broad range of industry segments including those trading in precious metals, including refiners; those trading in loose gemstones; large and small scale manufacturers of jewelry; and retail stores that function as a dealer in such items. **In addition, Treasury and FinCEN issued two advance**

**notices of proposed rulemaking seeking public comment on imposing an anti–money laundering program requirement on vehicle sellers and travel agents.** Section 352 requires Treasury to issue regulations requiring financial institutions to establish an anti–money laundering program that is commensurate with the financial institutions' size, location and activities.

Source: <http://www.ustreas.gov/press/releases/js43.htm>

[[Return to top](#)]

## **Transportation Sector**

**15. *February 21, Rocky Mountain News* — Chemical residue missed at DIA.** News4 in Colorado reported Thursday that **traces of explosive chemicals easily penetrated security checkpoints for passengers at Denver International Airport.** According to the report, the station used a "federally licensed explosives expert" to put traces of explosive chemicals on himself, his belt buckle, shoes and coat. He also put them on a carry–on bag and in a laptop computer and its case. On two occasions, the report said, the detector failed to pick up traces of the chemical. On another occasion, the passenger used by News4 was allowed to pass through the security checkpoint without using the swab to check him, the report said. **In all, nothing was detected four out of five times.**

Source: [http://rockymountainnews.com/drmn/local/article/0,1299,DRMN15\\_1760737,00.html](http://rockymountainnews.com/drmn/local/article/0,1299,DRMN15_1760737,00.html)

**16. *February 21, Agence France Presse* — Australia is "No. 4 on terrorists' hit list".** Australia is now fourth on the world's terror–attack hit list and **its flag carrier Qantas is most likely to be targeted**, the country's leading authority on terrorism warned on Friday. Clive Williams, director of terrorism studies at Canberra's Australian National University, told a security conference Australia's engagement in a war in Iraq would inevitably increase its profile. Williams told reporters at the conference in Brisbane that Australia's role in Iraq had implications for high–profile businesses, with Qantas, as possibly the best known business overseas. "Qantas has got a very good record in this area, they've always been very diligent about their security planning," he said. "They have probably done as much as they can do to safeguard their passengers." **He said all airlines would plan to divert flights away from Iraq and the Middle East in the event of war, a decision which would increase costs. A Qantas spokesman said the airline was in constant contact with security organizations in Australia and overseas and there were no signs Qantas was being singled out for a terror attack.**

Source: <http://straitstimes.asia1.com.sg/latest/story/0,4390,172996,00.html?>

**17. *February 20, PRNewswire* — ALPA criticizes TSA firearm carriage recommendation.** On Thursday, the Air Line Pilots Association (ALPA) criticized a key component of the Transportation Security Administration's (TSA's) preliminary Federal Flight Deck Officer (FFDO) program recommendations announced on Wed. The TSA has recommended that FFDOs carry a pistol in a holster while in the cockpit, but would require the pilot to secure and carry the pistol in a "lock box" secured in a flight bag or other container at all other times. "Congress created the FFDO program with the intention that airline pilots would be the last line of defense against airborne terrorism," said ALPA president Captain Duane Woerth. "In

passing the legislation, Congress mandated a program that would deputize airline pilots as federal Law Enforcement Officers (LEOs). Our members, most of whom have military and/or law enforcement backgrounds, will readily accept LEO training. However, they demand a TSA program that reflects their responsibilities, as well as their skills and professionalism. The horrible events of 9/11 identified the cockpit as a battleground and the need for qualified airline pilots to be trained as LEOs. **Congress specifically mandated that FFDOs be trained to ensure that the officer maintains exclusive control over his or her firearm at all times; the TSA's preliminary recommendation appears to thwart that statutory requirement."**

Source: [http://biz.yahoo.com/prnews/030220/deth055\\_1.html](http://biz.yahoo.com/prnews/030220/deth055_1.html)

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

## **Postal and Shipping Sector**

18. *February 23, Sun News (South Carolina)* — **Security measures safeguard port.** While area residents ship out to fight a possible war with Iraq, a coalition of forces in Georgetown, SC works to make sure the war doesn't hit too close to the Grand Strand. **Guarding a deep-water port, a power plant, a chemical plant and two major industries requires the daily coordinated efforts of the Georgetown County Sheriff's Office, the state Department of Natural Resources, U.S. Coast Guard, U.S. Customs Service and Department of Immigration and Naturalization.** Their aim is to make sure the port doesn't become a point of entry for terrorists or contraband and that ships and port facilities are safe from attack. **Georgetown Assistant Sheriff Carter Weaver said the Georgetown port is more vulnerable to attack because of the amount of commercial traffic it gets and its proximity to Charleston, one of the East Coast's busiest ports. A shortage of funding and additional patrol duties have put a strain on available resources,** though. The extra training, work hours and equipment used to tighten security have not been funded by the federal government. "That's an issue that the Coast Guard is trying to solve," said Michael Horan, a chief petty officer at the Georgetown Coast Guard Station. State-funded jobs also are feeling budget constraints. The state Department of Natural Resources lost 53 positions last year, at the same time it was being given more responsibility for port protection, spokesman Mike Willis said. **The DNR has done joint training with the Coast Guard on how to protect the port from terrorist attacks.**

Source: [http://www.myrtlebeachonline.com/mld/sunnews/news/local/5243\\_753.htm](http://www.myrtlebeachonline.com/mld/sunnews/news/local/5243_753.htm)

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

## **Agriculture Sector**

Nothing to report.

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

## **Food Sector**

19. *February 21, Clemson Tiger* — **Food packaging research prepares for combating potential bioterrorism threat.** Until recently, when most people consumed food or received packages,

they didn't think about threats to their safety. However, in light of the recent threats of bioterrorism, many are stopping to consider these issues more closely and are starting to analyze not only what they receive but also the package in which its contained. But this awareness is nothing new to several Clemson University researchers who work in the packaging science department. **For years the department has been working to develop packaging solutions for food safety and is now seeing ways to implement their research to protect the nation's food supply. Currently, Clemson researchers are devising new ways to preserve food for longer periods of time and also to indicate possible contamination or tampering through packaging technology.** First, scientists are testing package coatings that contain antimicrobial properties to defend against disease and bacteria. Other Clemson researchers are beginning to investigate indicator films that tell whether or not a product has spoiled or been contaminated by changing color.

Source: [http://www.thetigernews.com/vnews/display.v/ART/2003/02/21/3\\_e5583b688877](http://www.thetigernews.com/vnews/display.v/ART/2003/02/21/3_e5583b688877)

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

## Water Sector

Nothing to report.

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

## Public Health Sector

20. *February 21, Straits Times* — **New compound brings hope to TB patients. New Zealand scientists at Auckland University have found a compound that may provide a new cure for tuberculosis (TB). Laboratory tests in the United States have shown that the compound is effective against more than 50 strains of tuberculosis and other bacteria resistant to conventional antibiotics.** The U.S. National Institutes of Health agreed last week to use DNA testing to see how the compound worked. It could help save the lives of three million people worldwide who die of TB each year. Virulent forms of the disease, resistant to conventional drugs, are spreading in Asia, Africa, Europe, and the U.S. About 30 per cent of the world's population has been exposed to TB. **The compound will tried on animals, with results due within six to nine months. If successful, further trials on human TB patients could be fast-tracked under special U.S. Food and Drug Administration rules for infectious diseases, and drugs could be on the market within five years.**

Source: [http://straitstimes.asia1.com.sg/techscience/story/0,4386,17\\_2924,00.html](http://straitstimes.asia1.com.sg/techscience/story/0,4386,17_2924,00.html)

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

## Government Sector

21. *February 22, CNN* — **Al Qaeda hunt thwarts domestic terror.** Since the attacks on September 11, 2001, the FBI has doubled to 66 the number of joint terrorism task forces. Federal, state and local law enforcement agencies work closely together, sharing intelligence, informants and evidence. **Preventing attacks by foreign organizations is the top priority of the task forces but they also work on homegrown cases.** The FBI task forces have stopped a

Pennsylvania KKK leader who allegedly sought to set off grenades at abortion clinics, and a militant Jew who wanted to bomb a Southern California mosque and the offices of Lebanese-American Rep. Darrell Issa, (R-CA). The task forces also helped send to prison a white supremacist who plotted to blow up black and Jewish landmarks in Boston, Massachusetts and Washington. They were integral in the January 8 arrest in Chicago of Matt Hale, leader of the white supremacist group World Church of the Creator, on charges of trying to have a federal judge killed. **Intelligence officials say al Qaeda remains the primary threat for another major attack on U.S. soil, but they point out that even a single individual can wreak mayhem.**

Source: <http://www.cnn.com/2003/US/02/22/domestic.terrorists.ap/index.html>

22. *February 21, Washington Times* — **Watching like a hawk.** Customs officials say the two Black Hawk helicopters, running patrols over Washington since the national threat level hit Code Orange, will be flying missions over the capital for the foreseeable future. "We're definitely doing serious research into what it would entail to become a permanent presence here," Customs Officer William Oliver said of the patrols operating out of Ronald Reagan Washington National Airport. **As of Feb. 10, the two Black Hawks and two Cessna Citation airplanes flown by pilots with the Customs Service's Air and Marine Interdiction Division (AMID) are providing 24-hour patrols of airspace under 18,000 feet in roughly a 30-mile radius around the Washington Monument. A portion of the space is under scrutiny from the ground by the Army's Avenger missile systems placed in at least one strategic location near the Capitol. While commercial airline flights – monitored closely by the Federal Aviation Administration – are allowed into Reagan and Dulles International airports inside the restricted airspace, in the event that a small private aircraft enters the 30-mile radius it will be picked out by the Customs Service's Black Hawks or Cessnas. A Black Hawk will sneak up beneath the intruding plane, and if the aircraft doesn't quickly communicate and cooperate with customs pilots, the Department of Defense will be alerted. "If all else fails, and we think the guy is a threat, we call DoD (Department of Defense), they call Andrews Air Force Base, and Andrews will scramble a couple of F-16s," said Kevin Bell, a spokesman for the Customs Service.**

Source: <http://www.washingtontimes.com/national/20030221-88186895.htm>

23. *February 21, Washington Post* — **Analyst convicted in spy case.** A federal jury on Thursday convicted former Air Force intelligence analyst Brian P. Regan on three charges of attempted espionage, acquitted him on a fourth and said it could not agree on whether his spying should make him eligible for the death penalty. The panel was ordered to resume deliberation on that question Monday morning. **The 12-member jury found Regan guilty of trying to sell classified documents to Iraq and China and of breaking the law against gathering national defense information. Jurors rejected government arguments that Regan also tried to sell classified material to Libya, one of two counts that carried a possible death penalty. The Iraq charge was the other count punishable by death.** In a dramatic turn to a controversial case, jurors told the judge that Regan was guilty on the Iraq spying charge but said they disagreed over whether the crime met legal standards required to make him eligible for capital punishment. U.S. District Judge Gerald Bruce Lee sent the jurors home and ordered them to return Monday.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A37851-2003Feb 20.html>

24. *February 19, Associated Press* — **University, lab to work together on national security.** The University of New Mexico and Sandia National Laboratories plan to work together on research into policy issues linked to national- and international-security threats. **A new office for policy, security and technology will be created at UNM to focus on policy areas in which technology and security are related, such as weapons of mass destruction, arms control, terrorism and homeland security, the environment, energy, critical resources, borders and regional issues such as water scarcity.** The office will draw on the expertise of political science, economics and other social sciences as well as technical programs and Sandia, the university said. **The office will be funded at \$250,000 a year for five years by Lockheed Martin Corp., which runs Sandia for the U.S. Department of Energy. The goal is to make the office self-sufficient by creating support from corporations, policy foundations, government agencies and other institutions, Sandia said.**

Source: <http://santafenewmexican.com/site/news.cfm?BRD=2144461625AG=461>

[[Return to top](#)]

## Emergency Services Sector

25. *February 22, New York Times* — **Shoreline fire tests security plan of a city on edge.** In the minutes after the explosion, the **New York City Police Department initiated a plan to secure vulnerable parts of the city.** These include other fuel refineries and storage areas, landmarks, bridges, tunnels and other areas the police refer to as sensitive locations, like synagogues, hotels and other normally unguarded places. The Fire Department, after sounding a second alarm, broadcast a 10-60 code, which designated the explosion a major emergency; at one point, it dispatched four of the city's five elite rescue companies, at least two of the department's seven special squads, and the hazardous materials team. In addition, officials said, members of a special National Guard Weapons of Mass Destruction Civil Support Team, which is based in upstate New York but which came to the city two weeks ago in response to the national terrorism alert, went to the scene to test for chemical, biological and radiological agents. **Police officials said yesterday that the response to the explosion was an encouraging demonstration of how emergency resources should be deployed in a terrorism situation.** Police Commissioner Raymond W. Kelly, for example, said that under an order written early last year to ensure that police resources were not drawn in and overcome by any diversionary action, the department's response to the scene was limited. **But large numbers of officers were dispatched to dozens of sites – Kelly would not name them – that counterterrorism specialists consider particularly vulnerable.**

Source: <http://www.nytimes.com/2003/02/22/nyregion/22SECU.html>

26. *February 21, Post-Gazette* — **PEMA promises to find missing emergency equipment.** Pennsylvania Emergency Management Agency (PEMA) officials pledged yesterday to find out why a local anti-terrorism group has never received \$1.5 million worth of needed equipment even though the state received federal money for the gear back in 2000-01. **PEMA officials said the state was given money by the federal Office of Justice Programs to buy equipment for Pennsylvania's nine anti-terrorism work groups. But the homeland security group in southwest Pennsylvania -- the Region 13 Working Group -- has complained that they've never received the gear, said Shawn P. O'Connor, Knoll's spokesman.** "We are now aware of this problem and we're taking action," he said. "No one had

been looking into it." The Region 13 Working Group is a consortium of 13 southwest Pennsylvania counties and the city of Pittsburgh that meets once a month to coordinate anti-terrorism activities in the region. Knoll attended the group's regular meeting yesterday at the Allegheny County Emergency Operations Center in North Point Breeze.

Source: <http://www.post-gazette.com/localnews/20030221terror6.asp>

27. *February 17, Associated Press* — **State gets decontamination trailers.** Connecticut has acquired new tools to help respond to any terrorist attack – about two dozen 14-foot-high, 13,000-pound mass decontamination trailers. **The trailers would be deployed in the event of a biological or chemical emergency and are designed to get a contaminated person clean enough to be evaluated by medical personnel. Each trailer can process about 100 people in an hour.** The state acquired the trailers with a grant from the U.S. Department of Justice, said state police Sgt. John Vaz, who is with the state's Division of Homeland Security.

Source: <http://www.ctnow.com/news/local/hc-trailers0217.artfeb17,0,760102.story?coll=hc-headlines-local>

[[Return to top](#)]

## **Information and Telecommunications Sector**

28. *February 21, CERT/CC* — **CERT Advisory CA-2003-06: Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP).** The Session Initiation Protocol (SIP) is a developing and newly deployed text-based protocol that is commonly used in Voice over IP (VoIP), Internet telephony, instant messaging, and various other applications. **Numerous vulnerabilities have been reported in multiple vendors' implementations of the SIP. These vulnerabilities may allow an attacker to gain unauthorized privileged access, cause denial-of-service attacks, or cause unstable system behavior.** SIP-enabled products from a wide variety of vendors are affected. Other systems making use of SIP may also be vulnerable but were not specifically tested. Not all SIP implementations are affected. **Detailed instructions for resolving this issue may be found in this advisory on the CERT/CC Website. To determine if your product is vulnerable please refer to CERT/CC Vulnerability Note VU#528719 at <http://www.kb.cert.org/vuls/id/528719>**

Source: <http://www.cert.org/advisories/CA-2003-06.html>

29. *February 21, Wired* — **Hackers compromise security at AOL.** Hackers have compromised security at America Online, **potentially exposing the personal information of AOL's 35 million users.** The most recent exploit, launched last week, gave a hacker full access to Merlin, AOL's latest customer database application. **Merlin, which runs only on AOL's internal network, requires a user ID, two passwords and a SecurID code; hackers obtained all of these by spamming the AOL employee database with phony security updates, through online password trades, or by "social engineering" attacks over AOL's Instant Messenger (AIM) or the telephone.** Another **hole has allowed hackers to steal AIM screen names, even those of AOL staff members and executives.** Most at risk are screen names that hackers covet, like Graffiti, or single-word names like Steve. While many of these hacks utilize programming bugs, most hackers are finding it far easier and quicker to get access or information simply by calling the company on the phone. **These social engineering tactics involve calling AOL customer support centers and simply asking to have a given user's**

password reset. Logging in with the new password gives the intruder full access to the account.

Source: <http://www.wired.com/news/infostructure/0,1377,57753,00.html>

30. *February 20, Reuters* — **Swiss crack e-mail code, but minimal impact seen. Professor Serge Vaudenay of the Swiss Federal Institute of Technology in Lausanne, Switzerland, found a way to unlock a message encrypted using Secure Socket Layer (SSL) protocol technology, according to a posting on the research institute's Web site. However, U.S. cryptography experts said it was not the version of security that most consumers use to shop online. Rather, it is a version that only affects e-mail, is limited in scope, and not widely used, said Professor Avi Rubin, who is technical director of the Information Security Institute at Maryland's Johns Hopkins University. In addition, an attacker would have to be in control of a network computer located in the middle of the two people communicating over which the messages were flowing, he said. "It's possible, but it has limited applicability," he said. He said patches are already available to fix the hole, which affects one particular mode of OpenSSL. Like all co-called "open source" software, OpenSSL is free software created by developers who can modify it at any time. Bruce Schneier, chief technical officer at network monitoring firm Counterpane Internet Security, agreed. Besides the mitigating circumstances which lessen the likelihood that attackers would be successful, Schneier said SSL is irrelevant to security because attackers can more easily get at secret information while it is stored on computers and servers at the sending and receiving ends. "SSL protects the communications link between you and the Web" server, he said. "Nobody bothers eavesdropping on the communications while it is in transit."**

Source: <http://www.nytimes.com/reuters/technology/tech-tech-encrypti on.html>

31. *February 20, The Times* — **Firms in the United Kingdom warned of IT terrorists. Terrorist groups may try to infiltrate the computer systems of some of Britain's biggest companies, government departments and emergency services if a war is launched against Iraq, the Home Office of the United Kingdom has cautioned. Stephen Cummings, director of the National Infrastructure Security Co-ordination Centre (NISCC), said key IT systems were under threat of cyber attack by Islamic extremists. He said: "There will be groups attacking U.S. Government and defense websites and similar groups carrying out activity against the websites of any country involved in military action." Cummings urged businesses to step up security ahead of a possible war in the Gulf. He gave warning that terrorist groups might try to infiltrate activists into the IT departments of leading firms. "My view is that terrorist groups have identified the potential value in having people inside organizations rather than just responding passively as they have done in the past. There are already non-cyber examples of this," he said. Since NISCC was set up three years ago to monitor the threat of electronic attack against the UK, the number of digital attacks on "critical" organizations has soared. Cummings said that "there have been companies perceived to be in line with U.S. support for Israel in the past which have been attacked by pro-Palestinian groups. We could expect to see the same thing again from different sources."**

Source: <http://www.timesonline.co.uk/article/0,,5-584064,00.html>

Current Alert Levels	
 AlertCon: 1 out of 4 <a href="https://gtoc.iss.net">https://gtoc.iss.net</a>	 Security Focus ThreatCon: 1 out of 4 <a href="http://www.securityfocus.com">www.securityfocus.com</a>
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), 1434 (ms–sql–m), 80 (www), 4662 (eDonkey2000), 11044 (----), 4675 (eMule), 25 (smtp), 445 (microsoft–ds), 113 (ident), 0 (----) 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. *February 22, CNN* — **Border bust nets 10 tons of marijuana. In what is believed to be the largest–ever marijuana bust along America's southwestern border, U.S. Customs Service officers have seized nearly 20,000 pounds of marijuana from a tractor–trailer, officials said Saturday.** "This is a huge seizure," said Michael Turner, special agent in charge of the U.S. Customs office of investigations in San Diego. "Any time we can prevent 10 tons of narcotics from entering the streets of America, it's a great day for the U.S. Customs Service." In all, officials seized more than 4,000 packages weighing nearly 20,000 pounds. Customs agents estimated the marijuana's value at more than \$9 million. Customs agents arrested the truck driver, Carlos Ibarra, 39, of Tijuana, Mexico. The seizure tops previous marijuana busts in the Southwest. **In April 2001, customs officers intercepted more than 15,000 pounds of the drug at Otay Mesa. Earlier this month, officers found 12,600 pounds of marijuana at the El Paso, Texas, border station.**

Source: <http://www.cnn.com/2003/US/West/02/22/marijuana.bust/index.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.