



National Infrastructure Protection Center NIPC Daily Open Source Report for 22 January 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Hartford Courant reports that undercover inspectors twice smuggled a fake bomb in carry-on luggage past new federal baggage screeners at Bradley International Airport in November. (See item [7](#))
- Reuters reports security experts warn that global shipping faces unprecedented threats from Islamic militants linked to the al Qaeda terrorist network. (See item [11](#))
- The Washington Post reports the Federal Emergency Management Agency has published a 102-page handbook entitled "Are You Ready? A Guide to Citizen Preparedness," that explains how to prepare for and deal with terrorist acts as well as other man-made disasters. (See item [20](#))
- Computerworld reports cheap devices to jam Global Positioning System civil-use signals could also threaten military systems, since military GPS receivers must first acquire the C/A signal before locking onto the military signal, known as the P(Y) code. (See item [23](#))
- Government Computer News reports the National Cyber Security Leadership Act of 2003, that has been introduced to Congress, would mandate the use of IT security standards and guidelines established by the National Institute of Standards and Technology. (See item [24](#))

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. *January 21, The Miami Herald* — **Oil accidents mount in Venezuela. Venezuelan workers running the country's oil industry in place of striking employees and managers have caused at least 60 industrial accidents in the past month, including oil spills whose black stains stretch for a mile, local government leaders say.** The increase in spills and accidents is the direct result of blunders by inexperienced people running a dangerous and delicate business, according to striking oil workers, environmentalists and local government officials. Strike leaders say at least 4,500 barrels of oil have spilled and seven fires have broken out. **The accidents are one of the obstacles confronting the Venezuelan government as it faces a debilitating nationwide strike aimed at removing President Hugo Chávez from office. With about 35,000 of its 40,000 oil workers having walked off the job, the government disregards maintenance operations in its zeal to bring production back to normal levels, foreign diplomats monitoring the industry said.** Petróleos de Venezuela, S.A., known here as PDVSA, is leading a strike dubbed the "national civic stoppage," called Dec. 2 to force Chávez out of office. The strike has lasted far longer than anyone expected, and has cost the nation at least \$4 billion. While some strikers elsewhere have gone back to work, PDVSA remains devastated. Production, which had been at three million barrels daily, is down to about 600,000, though the government asserts it is nearly double that amount. And each day, more and more of that oil winds up at the bottom of Lake Maracaibo in the western state of Zulia, where tankers load cargo for international shipments. The Venezuelan government says the accidents have been exaggerated and are within industry norms. But even so, the government also blames sabotage by striking workers and the absence of security and maintenance personnel.
Source: <http://www.bradenton.com/mld/bradenton/news/world/4996794.htm>
2. *January 20, The Colorado Springs Business Journal* — **Wind power may be coming into its own.** Far lookers, seers and visionaries say renewable energy is not just something nice for the environment, but it may be a critical element in preserving a life as it is today. **They say wind power will play a big role in that picture, and projects in Colorado are already producing economically priced electricity. The Colorado Public Interest Research Foundation (CoPIRG) said in a special energy report that producing electricity from wind-powered turbines costs no more than that emanating from natural gas-powered plants.** The report is **Wind Energy, Powering Economic Development for Colorado.** It was released in Pueblo last month to a broad coalition of economic development directors, environmentalists, businesses, lawmakers, farmers and ranchers. CoPIRG says wind power is the new crop that will drive Colorado's electricity through wind-powered economic future. "Our research demonstrates wind energy is economical and good for our economy," said report co-author Stephanie Bonin. "Wind power is a new kind of crop Colorado's farming and ranching communities can toot for income...more wind energy means more jobs, more money for rural schools and a greener future for many farmers and ranchers in Colorado." **Another important aspect of wind-generated electricity is in the savings of billions of gallons of water annually used in hydroelectric production. Some said the current drought already affects the cost of hydroelectric prices.** In Colorado, the Golden-based National Renewable Energy Lab, owned by the U.S. Department of Energy, is developing new energy technologies in nearly 50 fields, and wind power has proven to be a viable source for future electrical needs. Colorado's utility companies will find a way to meet future need, CoPIRG said, but the question is in how. **"One path leads deeper into fossil fuel dependence with associated environmental and fuel costs ... the other path leads toward renewable energy supplies, cleaner air and water ... and reduced impacts from climate change,"** the report said. The

report is available from The Colorado Public Interest Research Foundation, 1530 Blake Street, Suite 220, Denver, CO. 80202.

Source: http://www.energycentral.com/sections/newsroom/nr_article.cfm?id=3581226

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

Chemical Sector

3. *January 21, Associated Press* — **Cyanide mining isn't banned—Senate committee kills bill.** A Colorado state Senate committee killed a bill Monday that would have restricted the use of cyanide to mine precious metals such as gold over the objections from residents who say the deadly chemical is endangering their lives. Ignacio Rodriguez, who has a home on the Alamosa River near Capulin, south of Monte Vista, said he first became aware of the danger when his horses refused to drink from the river. He said **tons of residue from cyanide mining still poses a danger to people downstream. Industry officials said banning cyanide would kill the gold mining industry in Colorado. They said cyanide was not to blame for polluting the rivers — it was the heavy metals from mining operations that caused the damage.** Sen. Ken Gordon, D–Denver, who sponsored Senate Bill 26, said he drafted the legislation after groups from across the state demanded the state prohibit any new open–pit cyanide gold mines. Colorado's first open–pit cyanide leach gold mine, the Summitville Mine, opened in 1986 over the protests of environmentalists. Several devastating cyanide spills followed and were blamed for killing aquatic life in the Alamosa River. Cleanup is expected to cost \$180 million. **The Legislature passed a law in 1993 to better regulate cyanide mining, but pollution problems continued.**

Source: http://www.bouldernews.com/bdc/state_news/article/0.1713.BDC_2419_1687982.00.html

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

Defense Industrial Base Sector

4. *January 27, Time* — **America's ultra–secret weapon.** Every war has its wonder weapon. In Afghanistan, it was the Predator, the unmanned drone that would loiter, invisibly, over the battlefield before unleashing a Hellfire missile on an unsuspecting target. The Gulf War marked the debut of precision–guided munitions, and in Vietnam helicopters came of age. World War II gave us the horror of nuclear weapons, and World War I introduced the tank. **If there's a second Gulf War, get ready to meet the high–power microwave or HPM. HPMs are man–made lightning bolts crammed into cruise missiles. They could be key weapons for targeting Saddam Hussein's stockpiles of biological and chemical weapons. HPMs fry the sophisticated computers and electronic gear necessary to produce, protect, store and deliver such agents. The powerful electromagnetic pulses can travel into deeply buried bunkers through ventilation shafts, plumbing and antennas. But unlike conventional explosives, they won't spew deadly agents into the air, where they could poison Iraqi civilians or advancing U.S. troops.** HPMs can unleash in a flash as much electrical power—2 billion watts or more—as the Hoover Dam generates in 24 hours. Capacitors aboard the missile discharge an energy pulse—moving at the speed of light and impervious to bad weather—in

front of the missile as it nears its target. That pulse can destroy any electronics within 1,000 ft. of the flash by short-circuiting internal electrical connections, thereby wrecking memory chips, ruining computer motherboards and generally screwing up electronic components not built to withstand such powerful surges. It's similar to what can happen to your computer or TV when lightning strikes nearby and a tidal wave of electricity rides in through the wiring. **Although the Pentagon prefers not to use experimental weapons on the battlefield, "the world intervenes from time to time," Defense Secretary Donald Rumsfeld says. "And you reach in there and take something out that is still in a developmental stage, and you might use it."**

Source: <http://www.time.com/time/covers/1101030127/nmicro.html>

5. *January 21, Defense Daily* — **Air Force halts GPS III program, competition put off until 2006.** The Air Force, citing budgetary constraints, is halting work on its Global Positioning System III (GPS III) program and delaying the competition for a prime contractor until at least 2006, industry officials reported last week. **Initially, the service was due to release a request for proposals for the final phase of competition in the program this month. However, competing contractors Lockheed Martin [LMT], Boeing [BA] and Spectrum Astro have all been informed that won't take place until 2006. The contract for the program is estimated to be as much as \$15 billion to develop and maintain a GPS satellite constellation and ground segment for 30 years.** The setback in the program comes as a surprise because Air Force leaders repeatedly have commented over the past years on the urgency for moving an enhanced, anti-jam GPS III capability to the field. The GPS III satellites are envisioned to have 100 to 500 times the anti-jam capability of current satellites. **While the Air Force has made the decision to hold off on GPS III, the notion may not fly when the budget request reaches Capitol Hill. Lawmakers in the past have been very adamant in pushing the Pentagon to upgrade its GPS capability to make it jam-proof.** "One question to be asked to the Air Force is how has the threat changed to justify the shorter program," one source said. Also, lawmakers have made it known in the past when they have not been pleased with the Air Force management of the program. While the Senate and House defense authorizers funded the \$102 million requested in FY '03 for the program, their appropriations counterparts slashed that to \$62 million. Some industry officials maintain that cut was made because the Air Force was not sending a clear signal to the Hill that the program was supported and well-planned out.

Source: <http://ebird.dtic.mil/Jan2003/s20030121147299.html>

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

Banking and Finance Sector

6. *January 17, Associated Press* — **Swiss bank watchdog sets tighter rules on money-laundering, terrorism.** The Swiss federal banking regulator Friday issued new rules to step up the fight against on money-laundering and terrorism by making banks and securities dealers increase efforts to spot and report wrongdoers. **The regulations, which take effect next July, require financial managers to increase surveillance of "higher-risk business relationships," the Federal Banking Commission said. The commission said the changes are in accordance with the directives of the Financial Action Task Force, the Paris-based organization that is coordinating the global fight against money laundering.** The Swiss

Bankers Association said the new ordinance demonstrates that a self-regulated banking industry can adopt "effective and tough rules for combatting criminal funds." **The regulations are the latest step in a series of measures that have been undertaken in recent years as Switzerland seeks to defend its banks from foreign criticism that they have been a haven for ill-gotten gains. The country has also been under pressure from the European Union to drop its banking secrecy, which the EU claims shields European tax dodgers.**

Source: http://story.news.yahoo.com/news?tmpl=storyp_woen_po/eu_gen_switzerland_money_laundering_1

[[Return to top](#)]

Transportation Sector

7. *January 21, Hartford Courant* — **Bradley International Airport security missed phony bombs. Undercover inspectors twice smuggled a fake bomb in carry-on luggage past new federal baggage screeners at Connecticut's Bradley International Airport in November, during a surprise security test that also saw an inspector successfully pass through with a knife taped to her leg, airport sources said.** The mock explosive was loosely modeled on the bomb, disguised as a radio, that was used to blow up a Pan Am 747 over Lockerbie, Scotland, in 1988. The sources said security managers briefed teams of screeners about the failed tests the next day, Nov. 19, during early morning roll calls. Dana Cosgrove, the federal security director at Bradley, would neither confirm nor deny reports of the failed tests. Federal authorities have no plans to make public the results of such tests at any specific airports nationwide. The screeners who reportedly missed the fake bomb at Bradley are employees of the federal government's newly formed Transportation Security Administration. Among the TSA's first priorities was to toughen qualifications for airport security jobs to improve safety. But early indications are that the new system has a long way to go to overcome past inadequacies. The General Accounting Office, the investigative arm of Congress, reported last summer that the TSA's surprise inspections around the country were not encouraging. **Belated discoveries of guns, knives and other potential weapons on passengers who had passed security checkpoints prompted evacuations of 124 airports since the TSA took over aviation security responsibilities last February, Dillingham reported. In those cases, 631 flights had been called back to terminals so passengers could be re-screened.** Dillingham said in an interview last week that he doesn't have more recent data on the performance of TSA screeners, but that he believes they are doing a better job than previous employees.

Source: http://www.ctnow.com/news/local/hc-bradbomb0121.artjan21.0.399049_story?coll=hc-headlines-local

8. *January 21, Wall Street Journal* — **Amtrak asks Congress for more assistance. Amtrak, while seeking \$1.2 billion from Congress to keep its trains operating this year, is quietly informing federal government officials it will need much more next year: \$1.5 billion to \$2 billion to start addressing long-neglected capital needs on its heavily traveled Northeast Corridor and other parts of the system.** The passenger railroad said **the higher funding levels are required to fix tracks and bridges on the corridor that connects Washington, New York and Boston and is Amtrak's busiest route.** Amtrak would also use the additional funds to purchase new cars and locomotives and to fix existing equipment. **Amtrak said the upgrades are necessary to reverse deterioration on the corridor and maintain it as a**

high-speed operation. David Gunn, Amtrak President and Chief Executive, said Amtrak has told the Office of Management and Budget in Washington that it will have to secure funds to replace about 70 miles of track that still have wooden cross-ties rather than modern concrete ties, rebuild decaying interlockings where trains switch from one track to another and replace several aged bridges on the corridor. The Northeast Corridor is Amtrak's fastest and busiest route, accounting for about 65% of Amtrak's passengers and including high-speed Acela Express trains, which are capable of running at 150 miles an hour but usually operate considerably slower due to infrastructure limitations on the corridor.

Source: <http://online.wsj.com/article/0..SB1043101823583235224.00.html?mod=home%5Fwhats%5Fnews%5Fus>

9. *January 21, Federal Computer Week* — **California installs wireless surveillance. The announcement last month that the California Department of Transportation (Caltrans) is putting wireless technology on several San Francisco bridges and tunnels for video surveillance may be just the beginning of a nationwide trend for such security measures.** In partnership with several contractors, Caltrans is installing a multimillion-dollar state-of-the-art wireless electronic surveillance system to enhance security. The system, called the Bay Area Security Enhancement, is operational and in the final phases of commissioning. **The secure system will enable state public safety agencies to monitor bridges and tunnels for potential security problems using cameras.**

Source: <http://www.fcw.com/geb/articles/2003/0120/web-bay-01-21-03.asp>

10. *January 17, Federal Transit Administration* — **Federal Transit Administration launches emergency preparedness forum in Newark. The Federal Transit Administration (FTA), will open its "Connecting Communities: Emergency Preparedness and Security Forum" in Newark, NJ on Jan. 22 – 23. The forums were created to help communities become better prepared to respond to emergency situations.** Using the successful evacuation of the transit stations below the World Trade Center as a benchmark, the goal of the forums is to demonstrate the important role that transit plays in crisis situations and the importance of delivering a coordinated regional response to any emergency. Participating transit agencies will work with regional emergency responders to determine the effectiveness of interagency response plans for the Newark region. **FTA's five-part Security Initiative includes evaluating threats and vulnerabilities through a security assessment; developing a plan to address vulnerabilities; testing the plan in realistic situations; training employees to understand and implement the plan; and undertaking research to enhance human capabilities.** Future scheduled forums are Feb. 5–6 in Los Angeles and Feb. 26–27 in San Diego.

Source: <http://www.dot.gov/affairs/fta0303.htm>

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

Postal and Shipping Sector

11. *January 21, Reuters* — **Expert says Islamic militants trained for sea attacks.** Global shipping faces unprecedented threats from radicals linked to Osama bin Laden's al Qaeda network who have been trained in suicide attacks developed by Sri Lanka's Tiger rebels, security experts said on Tuesday. **Suicide sea bombers are the latest addition to a growing**

list of threats facing the global shipping industry industry officials told a conference. The Maritime Intelligence Group, a Washington-based think tank, said members of a Southeast Asian Islamic militant group, the Jemaah Islamiah, had been trained in sea-borne guerrilla tactics developed by the Liberation Tigers of Tamil Eelam (LTTE), one of the world's most feared rebel armies. "We know that Jemaah Islamiah has benefited from the capabilities of the LTTE," Kweilen Kimmelman, a senior analyst at the Maritime Intelligence Group, told a conference on shipping security. **"They have had training in our estimation – certainly in terms of suicide diving capabilities and ramming." "Ramming" involves loading a boat up with explosives and steering it into a target.** It is one of several chilling techniques honed by the Tamil Tigers in their 19-year civil war against the Sri Lankan government. **Other attack methods include the use of "human torpedoes," underwater motor-propelled sleds used by divers to launch suicide attacks, along with deep-sea mines and small submarines.** "Ramming" is among the biggest worries for shippers after a small boat laden with explosives ripped through the French supertanker Limburg last October in the Gulf of Aden, killing a crewman in what Yemen called a "terrorist act." A similar attack in the Singapore and neighboring Malacca straits, a 1,000 km (621 mile) narrow stretch of waterway that is among the world's busiest shipping lanes and a vital lifeline between Asia and the rest of the world, could be devastating.

Source: <http://www.haaretzdaily.com/hasen/pages/ShArt.jhtml?itemNo=254625>
[ContrassID=80ont>](#)

12. *January 21, Canadian News Wire* — **Report urges increased financial support for Canadian port security. A recent study of port security in Halifax, Nova Scotia urges the federal government to give more financial support to the Royal Canadian Mounted Police (RCMP) and other security forces in their fight against terrorism.** The study, conducted by the Royal United Services Institute of N.S. (RUSI), included interviews with eight organizations involved in port security and operations. Bruce MacDonald, president of the Institute and one of three RUSI members involved in the study, said although **"local security authorities are well aware of the various threats and are doing a good job of ensuring security at the port, the resources at their disposal are not always sufficient to the task at hand."** **The several hundred thousand containers that pass through Halifax each year pose the main threat to port security, MacDonald explained.** The containers could contain weapons, conventional or nuclear, radiological, biological or chemical, that could be used in a terrorist attack here or elsewhere. **Such actions could disrupt transportation and transshipment services both in Canada and throughout North America.** At present, approximately three per cent of containers coming into Halifax are inspected. The planned introduction of a gamma ray machine, radiation detection equipment and a mobile X-ray machine in 2003 should help improve security, provided additional personnel and equipment are provided.

Source: <http://www.newswire.ca/releases/January2003/21/c1865.html>

13. *January 17, U.S. Customs Service* — **Republic of Korea signs declaration of principles to join U.S. Customs Container Security Initiative.** U.S. Customs Commissioner Robert C. Bonner and Yong-Sup Lee, Commissioner of the Customs Service of the Republic of Korea, announced on Friday that **the government of the Republic of Korea has agreed to participate in the U.S. Customs Container Security Initiative (CSI).** Commissioner Lee and Deputy U.S. Customs Commissioner Douglas M. Browning conducted the signing ceremony

on Friday, January 17, in Seoul. **Under terms of the declaration announced Friday, U.S. Customs officers will be stationed at the port of Busan.** "I am very pleased that the Republic of Korea has agreed to join with the United States in the Container Security Initiative," said Commissioner Bonner. "We recognize the high volume of trade between the Port of Busan and seaports in the U.S. and Busan's role as an intermodal transport hub for cargo originating in many countries. This is an important step, not only for the protection of trade between the U.S. and the Republic of Korea, but for the protection of the most critical component of the world trading system as a whole—containerized cargo."

Source: <http://www.customs.ustreas.gov/hot-new/pressrel/2003/0117-01.htm>

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

Agriculture Sector

14. *January 21, Japan Times* — Farm inspected over BSE discovery. Local health officials inspected the dairy farm in Hokkaido, Japan, Tuesday where the latest cow confirmed as carrying bovine spongiform encephalopathy (BSE) was born six years ago. The Holstein had been kept on a farm in Wakayama Prefecture and was discovered to have BSE in a routine check for the disease after being slaughtered last week for human consumption. **The diagnosis was confirmed Monday by a Health, Labor and Welfare Ministry panel, making it the sixth case of BSE in Japan since September 2001.** The fifth case was confirmed in August. During their inspection of the Shibechea farm, livestock officials from Kushiro, Hokkaido, asked about the feed being used by the farm and other cows born and raised there. After the investigation, officials hope to determine if there are any other cattle at risk of developing BSE the authorities said.

Source: <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20030122b2.h tm>

15. *January 20, Iowa Farm Bureau* — USDA triples number of BSE tests. The U.S. Department of Agriculture (USDA) more than tripled the number of cattle it tested for bovine spongiform encephalopathy (BSE) during the last fiscal year and has made significant steps on other prevention measures aimed at keeping the disease from entering the United States. In fiscal year 2002, USDA tested 19,990 cattle for BSE using a targeted surveillance approach designed to test the highest risk animals, including downer animals (animals that are non-ambulatory at slaughter), animals that die on the farm, older animals, and animals exhibiting signs of neurological distress. During FY 2001, USDA tested 5,272 cattle. Both figures are significantly higher than the standards set by the Office International des Epizooties (OIE), the standard setting organization for animal health for 162 member nations. Under the international standard, a BSE-free country like the United States would be required to test only 433 head of cattle per year.

Source: <http://www.ifbf.org/publication/spokesman/story.asp?number=20495&type=Ag>

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

Food Sector

Nothing to report.

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

Water Sector

Nothing to report.

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

Public Health Sector

16. *January 21, Boston Globe* — **Free antiradiation pill supply exceeds demand. One year after Massachusetts became the first state to order radiation–protection pills for nuclear power plant neighbors, and six months after it began offering the pills for free, about 80 percent of the tablets remain locked up in a storeroom at the state pharmacy in Tewksbury. Many other pills remain undistributed in local pharmacies. Despite the headlines Massachusetts earned from its first–in–the–nation decision, the pills were offered at pharmacies and town offices for only two months and then quietly withdrawn. In such dire fiscal times, it's difficult to find money to promote antiradiation pills, said Robert Walker, director of the Radiation Control Program at the state Department of Public Health. The government can only provide the pills, which are also known by the chemical shorthand KI. It cannot require people to pick them up, Walker said.**

Source: http://www.globe.com/dailyglobe2/021/metro/Free_antiradiation_pill_supply_exceeds_demand+.shtml

17. *January 20, Pacific Northwest National Laboratory* — **Antibody library speeds search for new detection tools. Scientists at the Department of Energy's Pacific Northwest National Laboratory (PNNL) have extracted part of the human immune system and reconstituted it in brewer's yeast in a fashion that enables powerful machines to quickly identify new antibodies. The advance could have major repercussions for fundamental biological science as well as industries that use antibodies for sensors, biodetectors, diagnostic tools, and therapeutic agents.** The technology could replace the need to produce antibodies within animals, such as mice, and opens up new possibilities for rapidly designing medical treatments more acceptable to the human immune system. Antibodies are proteins produced by white blood cells as part of the immune response. "Our antibody library offers many advantages over traditional approaches. We expect it will be a more effective tool for scientists," said Michael Feldhaus, PNNL scientist. Feldhaus and colleague Robert Siegel built a library of 1 billion human antibodies and expressed them on the surface of yeast cells using a platform designed by collaborator Dane Wittrup of the Massachusetts Institute of Technology. **The combined technologies offer a more powerful, less expensive method for identifying antibodies.**

Source: <http://www.pnl.gov/news/2003/03-01.htm>

18. *January 20, USA Today* — **Hospitals decline smallpox vaccine. More than 80 hospitals from every region in the United States, including leading teaching hospitals and large, urban public hospitals, are forgoing the vaccinations.** The dissenters are a tiny fraction of the 3,000 hospitals recruited by state health officials to vaccinate doctors, nurses and other hospital staff members who are most likely to care for smallpox patients. Their numbers are growing as doctors and administrators at hospitals around the U.S. are concluding that the

known health risks from the vaccine, which can cause illness and even death, outweigh the unquantifiable risks of smallpox being used as a terrorist weapon. The hospitals are reaching their decisions individually after their own in-house infectious disease specialists study the Bush plan. Almost as a rule, hospital administrators say they are reluctant to make some of their employees sick to protect them from a disease that no longer exists and would reappear only in the chance of a terrorist act. **The Bush administration plans to vaccinate 440,000 frontline health care workers within the next four to six weeks and then begin vaccinating 10 million additional health care workers, police officers, firefighters, and other emergency personnel by late summer.** The program for health care workers is voluntary. The count of the hospitals taking a pass was conducted by USA TODAY in a telephone survey of public health officials in all 50 states and selected cities and should be considered a conservative estimate. **Many officials were unable to provide specifics because hundreds of hospitals around the country have not yet decided what to do.** Nonetheless, the phone survey shows scattered opposition to smallpox vaccinations before an attack. Hospital chains in Charlotte, N.C., and Denver are taking a pass, as well as hospitals in Atlanta, San Francisco and suburban Minneapolis. **Additionally, some hospitals participating in the plan report that many of their employees are declining to be vaccinated. "There aren't a lot of people volunteering," says Susan Fernyak, director of communicable-disease prevention at the San Francisco Department of Public Health. "If you look at the guidelines for a moderate hospital, 100 to 150 people would be vaccinated. But even at the larger hospitals, there aren't going to be that number of volunteers."**

Source: http://www.usatoday.com/news/health/2003-01-20-smallpox-cover-usa_t_x.htm

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

Government Sector

19. *January 21, Del Moines Register* — **Security spending called 'overkill'.** Iowa lawmakers, concerned that unquestioned homeland security spending has gone too far, are scrutinizing **the proposed installation of more than 100 surveillance cameras in state buildings and the purchase of about 1,000 "smart" employee identification cards at more than \$20 each.** About \$500,000 has been spent on a control center to monitor surveillance cameras and other security systems at the Capitol and state office buildings. **Twenty-eight of the cameras are in place, but about 120 more would be required to provide full coverage of buildings and parking lots.** Members of the Legislative Oversight Committee have asked state officials to suspend security upgrade plans because of concerns about their cost during tight budget times. **Since the terrorist attacks of Sept. 11, 2001, the Legislature has approved \$1.3 million to increase security at the Capitol complex.** Critics complain that the state has overreacted to threats of terrorism and workplace violence. "It's overkill," said Sen. Jack Hatch, a Des Moines Democrat. The National Governors' Association estimated the states' first-year cost of homeland security measures at \$4 billion, with most of the spending devoted to bioterrorism preparedness and emergency communication equipment. **In Iowa, legislators have been squeamish about questioning purchases of security gear because they don't want to be seen as opposing homeland security, but that attitude seems to be changing, Hatch said. State officials, including Public Safety Commissioner Kevin Techau, say they support a reassessment of security requirements. His officers patrol the Capitol grounds and monitor cameras and alarm systems.**

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

Emergency Services Sector

20. *January 21, Washington Post* — **FEMA issues emergency planning book.** The federal government has recently issued a guide to tell individual citizens how to prepare for disaster. **The safety guide by the Federal Emergency Management Agency (FEMA) explains how to prepare for and deal with terrorist acts as well as other man-made disasters — such as hazardous waste accidents — and natural catastrophes. The 102-page handbook, "Are You Ready? A Guide to Citizen Preparedness," presents strategies for dealing with everything from tornadoes and heat waves to toxic spills and suspicious packages. The guide also gives information on crisis counseling, disaster plans and even what to do about animals in a disaster.** One of the handbook's main suggestions, FEMA Deputy Director Michael D. Brown said, is for people to create disaster supply kits for the home, workplace and vehicle. The kits should include supplies of water, food, first-aid equipment, clothes, bedding, emergency materials, kitchen and sanitation items, household documents and contact numbers. The guide also explains how to build a temporary fallout shelter that could house you for a few days to as long as a month in the event of a radiological attack. Since the Sept. 11 attacks, Brown said, people have shown a strong desire for emergency preparedness information. "After 9/11 there was a huge spike of interest," Brown said, "and what we're really trying to do is capitalize on that spike of interest." **"Are You Ready?" is available on the FEMA Web site, www.fema.gov. Officials still are deciding how to distribute the first 100,000 copies across the nation, Brown said. An additional 100,000 copies are scheduled for distribution in about a month, and Spanish-language versions should be ready by mid-March, according to the agency.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A18994-2003Jan20.html>

21. *January 19, New York Times* — **New York state misses two deadlines on security plans.** When the Federal Emergency Management Agency (FEMA) pledged \$8.8 billion to help New York City rebuild after Sept. 11, 2001, it set aside a minimum of \$418 million for the state to finance projects to bolster the metropolitan area's preparedness for any future terrorist attack. **But in the 16 months since the attack that destroyed the World Trade Center, the state has not submitted a single project for FEMA to review, even though it has received scores of proposals from state, city and private agencies desperate to do everything from reinforcing bridges to shoring up bioterrorism efforts at local hospitals. In fact, the state has missed two deadlines for submitting the proposals, and has been forced to ask for two extensions totaling six months — requests that emergency management officials say have been rare in other disasters.** The failure so far to take advantage of hundreds of millions of available dollars when both the state and city are in fiscal crises has troubled many local elected officials, Democrats and Republicans alike, who worry that the delays and indecision will hurt the state's ability to make a case for any money in the future. **State officials attributed the delays in part to the complexity of deciding how best to protect against terrorists capable of sophisticated and varied assaults. They also said that simply sifting through all the proposals, with costs totaling an estimated \$6 billion, has taken an enormously long time. "A project of this magnitude is far too important to rush," said Mollie Fullington, a**

spokesperson for Gov. George E. Pataki. "The terrorist attacks on America were an unprecedented disaster, and this application clearly does not fit within the confines of a typical time period to prioritize projects for these funds."

Source: <http://www.nytimes.com/2003/01/19/nyregion/19FUND.html>

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

Information and Telecommunications Sector

22. *January 21, Associated Press* — **Software to snag hackers in real time.** Recent data intrusions, whose authors are typically intent on theft, sabotage or cyberterrorism, have given rise to a promising profiling—and-reasoning strategy aimed at preventing online break-ins as they happen. Researchers at the State University of New York at Buffalo are developing "user-level anomaly detection" software that draws up regularly updated profiles by closely tracking over time how each person performs an array of routine tasks, such as opening files, sending e-mail or searching archives. The system could provide a high-grade layer of protection for military installations and government agencies as well as on commercial networks. Designed to tell if someone has strayed into an unauthorized zone or is masquerading as an employee using a stolen password, the program keeps watch for even subtle deviations in behavior. Alerted to anomalies, network administrators then begin monitoring more aggressively to assess whether pilferage is in progress.

Source: http://www.businesstoday.com/business/technology/ap_hack01212003.htm

23. *January 20, Computerworld* — **GPS jammers raise concern.** The current issue of the online hacker magazine Phrack provides directions for making cheap devices to jam Global Positioning System signals (GPS). The article says the jammer was designed to work only against GPS civil-use signals broadcast on the frequency of 1575.42 MHz and not the military frequency of 1227.6 MHz. However, James Hasik, a consultant, said that while the jammer was targeted against the civil GPS signal, known as the C/A code, it could also threaten military systems, since "almost all military GPS receivers must first acquire the C/A signal" before locking onto the military signal, known as the P(Y) code. **The Department of Defense (DOD), which faces the possibility of its GPS-guided weapons encountering Russian-made GPS jammers in Iraq, has antijamming technology at its disposal.** Air Force Lt. Col. Ken McClellan, a Pentagon spokesman, said GPS experts at the Pentagon don't "at the moment" view homemade jammers as a hazard to safety of flight for civil aircraft or ship operations, "but rather a nuisance." **The Federal Aviation Administration (FAA) is developing a nationwide GPS-based precision landing system. And the U.S. Coast Guard (USCG) operates a GPS-based maritime navigation system.** Bill Mosley, a spokesman for the Department of Transportation (DOT), the parent agency of the FAA and the USCG, said his department is well aware of the threat posed by GPS jammers.

Source: http://www.computerworld.com/securitytopics/security/story/0,1080_1,77723,00.html

24. *January 20, Government Computer News* — **National Cyber Security Leadership Act of 2003 introduced to Congress.** Senator John Edwards (D-NC) has introduced a bill that would require agency CIOs to identify significant vulnerabilities in IT systems; establish performance goals for eliminating the weaknesses; and evaluate performance at least quarterly. **The National Cyber Security Leadership Act of 2003 would also mandate the**

use of IT security standards and guidelines established by the National Institute of Standards and Technology (NIST). The bill, introduced January 16, has been referred to the Senate Governmental Affairs Committee. **NIST would be charged with developing guidelines within six months to address the vulnerabilities.** The guidelines could become mandatory unless agencies received exemptions. **The bill complements the Federal Information Security Management Act (FISMA), which was incorporated in the Homeland Security Act of 2002.** FISMA requires agencies to assess risks to IT systems and to provide "information security protections commensurate with the risk." It also requires development of security programs, annual evaluations of the programs and annual reports to OMB.

Source: http://www.gcn.com/vol1_no1/daily-updates/20899-1.html

Internet Alert Dashboard

| Current Alert Levels | |
|--|---|
|  AlertCon: 1 out of 4 https://gtoc.iss.net |  Security Focus ThreatCon: 1 out of 4 www.securityfocus.com |
| Current Virus and Port Attacks | |
| Virus: | #1 Virus in the United States: WORM_KLEZ.H Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States] |
| Top 10 Target Ports | 137 (netbios-ns), 80 (http), 1433 (ms-sql-s), 445 (microsoft-ds), 4662 (???), 139 (netbios-ssn), 53 (domain), 8714 (???), 3389 (ms-term-serv), 23 (telnet) Source: http://isc.incidents.org/top10.html ; Internet Storm Center |

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

General Sector

25. *January 23, The Brookings Institution* — **Protecting the American homeland: a second look at how we're meeting the challenge.** On the eve of the new Department of Homeland Security officially opening for business, a group of Brookings scholars examines the question: **Will Americans be any safer as a result? In a follow-up appraisal to their earlier report "Protecting the American Homeland," they conclude that at some future point the department may increase security against terrorist attacks on the American homeland, but not immediately.** In 2002, according to the report, America lost momentum on improving homeland security. While the primary focus of Washington policymakers in the second half of the year—creating the Department of Homeland Security—may have some merit, the managerial challenges confronting Homeland Security Secretary Tom Ridge and his staff are extraordinary. **Most worrisome, say the authors, is that the complexity of merging so many**

disparate agencies threatens to distract policymakers from other, more urgent security efforts. Congress has still not passed a federal budget for homeland security for fiscal year 2003, which began on Oct. 1, 2002, and last summer, President Bush vetoed several measures proposed by Congress that would have addressed critical national vulnerabilities. The report asserts that as a result, America remains more vulnerable than it should be on the eve of a possible war against Iraq, which could inspire more terrorist attacks.

Source: <http://www.brookings.edu/comm/events/20030123.htm>

[[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 Advisories](#) – Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

[NIPC Alerts](#) – Alerts address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

[NIPC Information Bulletins](#) – Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

[NIPC CyberNotes](#) – CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

NIPC Daily Open Source Report Contact Information

| | |
|--------------------------|--|
| Content and Suggestions: | Melissa Conaty (202-324-0354 or mconaty@fbi.gov) Kerry J. Butterfield (202-324-1131 or kbutterf@mitre.org) |
| Distribution Information | NIPC Watch and Warning Unit (202-323-3204 or nipc_watch@fbi.gov) |

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.