



National Infrastructure Protection Center NIPC Daily Open Source Report for 13 January 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The New York Times reports current emergency plans are inadequate to protect the public from a disastrous leak of radiation at the Indian Point nuclear plant in Westchester County and do not fully take into account the possibility of a terrorist attack. (See item [2](#))
- The Associated Press reports the U.S. Customs Service has announced that starting next month, sea carriers must provide details of the contents of sea containers destined for the U.S. 24 hours before the cargo is loaded onto ships at foreign port. (See item [9](#))
- International Data Group reports Microsoft has announced an Internet routing error by ATTshut off access from around 40 percent of the Internet to several major Microsoft Web sites and services on Thursday. (See item [20](#))
- The Washington Times reports officials are considering faster ways to alert U.S. to terrorism using the Emergency Alert System. (See item [21](#))

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 12, CNN* — OPEC to raise daily oil output. OPEC is to boost oil output target by 1.5 million barrels a day to 24.5 million barrels a day. The increase will take effect on February 1, OPEC President Abdullah bin Hamad Al Attiyah told a news conference. "OPEC is trying to send a very strong message that it will do its utmost to stabilise demand and supply," Al Attiyah was quoted by the Associated Press. United Arab Emirates

Oil Minister Obaid bin Saif al-Nasseri said the increase amounted to a rise of seven percent. The decision was taken on Sunday after OPEC leaders met to discuss raising oil production in a bid to slow rising prices amid fears of supply problems caused by an ongoing strike in Venezuela. The six-week old strike by political opponents seeking to oust President Hugo Chavez has forced a cut in the country's exports by about two million barrels a day. **Venezuela is normally the third-largest producer among members of OPEC -- Organization of Petroleum Exporting Countries -- and a major oil supplier to the United States.**

Source: <http://www.cnn.com/2003/BUSINESS/01/12/opec.meeting.lead/index.html>

2. *January 11, New York Times* — **Nuclear plant disaster plan is inadequate, report says.**

Emergency plans are inadequate to protect the public from a disastrous leak of radiation at the Indian Point nuclear plant in Westchester County and do not fully take into account the possibility of a terrorist attack, according to a 500 page report commissioned by Gov. George E. Pataki and released yesterday. **Contrary to repeated assurances from state and federal officials in the past, the report said the plan was "not adequate" to "protect the people from an unacceptable dose of radiation in the event of a release from Indian Point, especially if the release is faster or larger" than currently anticipated.** It said that the plan, created by the state, the counties surrounding the plant, and Entergy, the plant's owner, assumes an accidental release rather than a deliberate release from an attack. **Although federal officials predict that most deaths would occur within a 10-mile radius of the plant, radiation sickness and possible contamination of food and water could spread to 50 miles from it, an area of 20 million people that includes New York City, according to the Nuclear Regulatory Commission.** "Simply stated, the world has recently changed," said the report, by James Lee Witt, a private consultant and former director of the Federal Emergency Management Agency. "What was once considered sufficient may now be in need of further revision." Witt was not asked to consider whether the plant should be shut down, a step that a range of public officials, environmentalists and residents have sought, particularly since Sept. 11, 2001, when one of the hijacked jets flew near the plant on its way to the World Trade Center. He was also not asked to look into the operation or safety of the plant itself. The current disaster plan focuses on the 298,013 people who live within 10 miles of the plant and would be most affected by a disaster. Although the report said the state should take into account people evacuating on their own outside of that 10-mile radius, it did not suggest that wholesale evacuation plans be developed for more distant places like New York City. **The report also examined plans on Long Island for a disaster at the Millstone nuclear plant on the Connecticut shore but found that they "should be able to protect" the public.** Governor Pataki, who ordered the report last August in response to the rising outcry over safety at the plant, declined to comment on it beyond a statement calling on federal authorities to review their standards for emergency plans "and determine if they are strong enough to meet the post-Sept. 11 reality."

Source:

<http://www.nytimes.com/2003/01/11/nyregion/11NUKE.html?ei=10fb21e9a03f4begewanted=print>

3. *January 09, UtiliPoint International* — **Enthusiasm for transmission lines down.** As an increasing number of electricity providers are scheduling power deliveries over the transmission system, more problems are starting to surface. **Not only is the capacity inadequate to support the demand but the infrastructure is quickly becoming outdated. The result is that reliability has been called into question.** But new transmission is not getting built at the pace that is necessary. **The difficulties in winning permits coupled with lack of capital flowing to such projects means that less expensive generation may sit idle**

because of inadequate or congested transmission lines. ISO New England, operator of the region's bulk electric power system, for example, says that about \$900 million is needed for upgrades to maintain reliability and efficiency. More than 30 transmission projects have been planned or proposed by electric companies in the Northeast. According to Gordon van Welie, chief executive officer for ISO New England, roughly 4,500 megawatts of new generation has been added to the region's power system over the past three years, yet similar investment in the region's transmission system has not occurred. **"As a result, the region's power system and wholesale power exchange are operating below optimum efficiency,"** he says. "The economic value of New England's transmission congestion costs is currently estimated to range from \$50 to \$300 million, while the economic consequences of system blackouts in highly stressed areas such as southwest Connecticut are incalculable." Between 1979 and 1989, transmission capacity grew at a slightly faster rate than the demand for electricity during peak periods. But in the subsequent decade, infrastructure needs did not keep up with that demand—a phenomenon that still persists. **To handle the requirements that the transmission system expects over the next 10 years, about \$56 billion will be necessary, says the Edison Electric Institute (EEI), noting that 27,000 gigawatt–miles are required. However, only 6,000 gigawatt–miles are planned.** It has all led to more congestion and less efficient electric prices. Congestion grew by 200 percent between August 1999 and August 2000. And in the first quarter of 2001, congestion was three times the level experienced in all of 2000. A study by Electric Power Research Institute (EPRI) concluded that more than \$45 billion is lost annually to outages and another \$6.7 billion to power–quality disturbances, which necessitates the building of new transmission lines as well the upgrading of aging ones.

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=UtiliPoint+International_2003_01_09_1042146040850tentSet=0

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

4. *January 13, Jacksonville Daily New* — **Local, state and federal officials gathered at the Camp Lejeune Marine Corps base to discuss a plan for responding to a nuclear emergency.** While an extensive force of Camp Lejeune Marines began deploying for a potential war with Iraq — local, state and federal officials gathered at the Marine Corps base to discuss a plan for responding to a nuclear emergency. Firefighters, law enforcement officers and emergency personnel, all part of the Military and Civilian Task Force for Emergency Response, attended Saturday's workshop to discuss that possibility with national experts. If the ideas they develop are successful, the project could be used to protect various cities and military installations throughout the country, said Mark Goodman, Onslow County Emergency Services director. One of the goals is to stop any radiological incidents from happening by developing technology that will detect the material before it reaches the area. Camp Lejeune was one of four permanent pilot programs chosen to provide an equipment list and procedures for protecting important sites such as military bases from weapons of mass destruction.

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

Banking and Finance Sector

5. *January 10, New York Times* — **Agency to expand units tracing terrorist finances.** Federal officials, worried that terrorist financing links in the United States are more pervasive than previously thought, said thursday that they had decided to double the size of the operation devoted to rooting out terrorist-tainted money. **The expansion, coming after several major breaks in terror financing cases in recent weeks, reflects a realization by customs authorities that they need more investigators, greater resources and a reorganized structure to shut down the pipeline that finances terrorism.** Investigators for the Customs Service's terrorist financing operation, which has assumed the lead role for such cases since Sept. 11, 2001, have become so bogged down in leads and evidence – one set of search warrants produced 550 boxes of documents – **that officials are expanding their personnel to 460, from about 240. Customs plans to redeploy at least 150 investigators to terrorist financing from other assignments and will be asking partner agencies, like the Federal Bureau of Investigation and the Internal Revenue Service, to commit more agents as well. At the same time, the Customs Service will create 14 additional teams next Monday in cities around the country to investigate terrorist financing full time, officials said.**

Source: <http://www.nytimes.com/2003/01/10/politics/10LINK.html>

6. *January 10, Wall Street Journal* — **Bush Administration to push for identity-theft measures.** Administration officials want to take advantage of the expected reauthorization this year of certain provisions in the Fair Credit Reporting Act to create new protections for victims of identity theft. For identity-theft victims, "it often will take you months, in some cases years, and thousands of dollars to correct your record, and that's just unacceptable," said Wayne Abernathy, the newly confirmed assistant Treasury secretary for financial institutions. **A provision of the Fair Credit Reporting Act gives national standards on information sharing by financial companies primacy over state law. When the provision expires this year, the Bush administration wants to reauthorize it, with changes. Without a new provision, states might pass laws aimed at protecting financial privacy that impair the data-sharing necessary for financial companies to verify a customer's identity, Mr. Abernathy said. At the same time, "this really gives us an opportunity to deal with this [identity theft] issue."**

Source: <http://online.wsj.com/article/0..SB1042160410638415664.00.html>

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

Transportation Sector

7. *January 10, Washington Post* — **Expect a bad year, airlines tell Senate. The airline industry will suffer another unprofitable year and does not expect to recover until 2004, executives of the major U.S. carriers told members of Congress Thursday.** In a hearing before the Senate Committee on Commerce, Science and Transportation, the executives said the industry's

outdated cost structure needs an overhaul to ensure the major airlines' survival. They said they particularly need to reduce labor costs and heard some support for a revision in the labor law that would limit strikes. **Richard H. Anderson, chief executive of Northwest Airlines, said he expected the industry to lose about \$3 billion this year, after a loss of \$9 billion in 2002. "The airline industry remains stuck in the most difficult period of financial distress it has suffered since it was deregulated almost 25 years ago, perhaps the most difficult period in modern aviation history,"** said Jeffrey N. Shane, an associate deputy secretary of transportation. American Airlines chairman and chief executive Donald J. Carty pointed to several forces that are driving the larger airlines to restructure their operations. In addition to the fallout from the September 2001 terrorist attacks, the big airlines have had to confront the rapid expansion of low-cost carriers, the increasing use of the Internet by travelers looking for cheap fares, and the reluctance of business travelers to pay several times what leisure travelers pay for a flight.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A35262-2003Jan9.htm>

- 8. *January 09, Transportation Security Administration* — Chicago O'Hare to require boarding passes at checkpoint starting Friday, Jan. 10.** Under Secretary of Transportation for Security Adm. James M. Loy today announced **Chicago O'Hare International Airport (ORD) is joining 57 other airports in participating in the Transportation Security Administration's "Selectee Checkpoint" program, which enhances security and convenience by transferring the screening of selectees from aircraft boarding gates to security checkpoints where screening equipment and personnel and law enforcement officers are concentrated. At these airports, passengers must now have their boarding passes in hand before they reach the checkpoint.** E-ticket receipts, itineraries and vouchers will no longer provide access through the checkpoints, and boarding passes will no longer be issued at the gates. Boarding passes may be obtained at ticket counters, through airline computer kiosks, or at sky cap curbside stations. In addition to a boarding pass, passengers must show a valid government issued photo ID, such as a driver's license or passport at the checkpoint. Checkpoints at these airports have been reconfigured to channel selectees through a special lane.

Source: <http://www.dot.gov/affairs/tsa0403.htm>

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

Postal and Shipping Sector

- 9. *January 10, Associated Press* — Rule requires U.S.-bound cargo details.** Starting next month, sea carriers must provide details of the contents of sea containers destined for the U.S. 24 hours before the cargo is loaded onto ships at foreign ports, the chief of the U.S. Customs Service said Thursday. **Customs Commissioner Robert Bonner put carriers and shippers on notice that the service will begin enforcing the rule on Feb. 2 as originally planned. The rule was put in place Dec. 2 with a 60-day grace period, giving sea carriers time to come into compliance.** Although no formal requests were made to the agency to extend the grace period, Bonner said that informally there have been rumblings among some carriers hoping for more time. "We can't roll this back any further," he said. **Companies that fail to provide accurate manifest information 24 hours before loading could be barred from unloading cargo containers at a U.S. port and could be fined, Bonner said.** Carriers making a "good

faith" effort to comply with the rule would – at the beginning at least – be given leeway to correct minor shortcomings before being hit with such penalties.

Source: <http://www.guardian.co.uk/uslatest/story/0,1282,-2309387,00.html>

10. *January 09, Press-Telegram* — **Long Beach port to test new ID cards. Truckers, longshoremen and other workers at Long Beach, California waterfront terminals soon may be required to carry new ID cards as part of a plan to beef up port security.** As part of a new pilot program, **the Port of Long Beach will test digital and holographic photo identity cards with an embedded electronic chip, magnetic strip, bar code and an optical laser strip.** The pilot project will test the different technologies to determine which works best. **The Transportation Security Administration is also developing a similar program, albeit on a smaller scale, at some East Coast ports.** A three-phase process will be used to select and evaluate technologies so that a prototype worker identity card system will be in place by the end of the year, according to port officials.

Source: <http://www.presstelegram.com/Stories/0,1413,204%257E21474%257E1100313,00.html>

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

Agriculture Sector

11. *January 10, Nature.com* — **Foot and mouth strategy strengthened. An antiviral drug could avert future foot-and-mouth disease (FMD) epidemics, scientists say. Combined with vaccination, the drug gives slow-acting vaccines time to kick in.** More than 6 million animals were slaughtered in 2001 as Britain struggled for 7 months to stop FMD tearing through farmyards. **Vets shunned animal vaccination because the virus jumps from herd to herd before vaccines can take effect. The antiviral drug interferon protects pigs from infection for at least 24 hours, says Marvin Grubman of Plum Island Animal Disease Center in Greenport, New York. Crucially, it starts working within a day. "No vaccine can protect animals so quickly," he says. "It's potentially hugely significant,"** agrees FMD epidemiologist Mark Woolhouse of the University of Edinburgh, UK. At the time of the British outbreak, experts favoured culling over vaccination. Taking 7 days to provide immunity, a vaccine strategy might have worsened the epidemic, they feared. Recent inquiries such as those by Britain's Royal Society have recommended well-planned emergency vaccination – alongside culling – should FMD return. "This finding tips the balance towards vaccination," says Woolhouse.

Source: <http://www.nature.com/nsu/030106/030106-14.html>

12. *January 10, Food Production Daily* — **War on E.coli. Beef industry leaders meeting in the U.S. this week have formulated an action plan to fight the war against Escherichia coli O157:H7 in the beef supply and committed to a series of industry-wide actions to move them toward this goal.** More than 200 industry leaders, representing each link in the beef production chain, participated in a two-day working summit that was sponsored by the National Cattlemen's Beef Association. The summit focused on identifying good manufacturing practices, interventions and research needs to reduce the incidents of E. coli. Action steps were identified for each industry segment: cattle production, fabrication, processing, retail and foodservice. **Specific actions recommended include: expanded research and fast-tracked**

approval of interventions such as cattle vaccines and feed additives; standardisation of safety testing and verification at packing plants; uniform practice of sampling, testing and negative confirmation before meat processing; microbial control systems for foodservice suppliers; consumer information regarding cooking temperatures and thermometer use at point of purchase.

Source: <http://www.foodproductiondaily.com/news/news.asp?id=1989>

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

Food Sector

13. *January 10, Associated Press* — **Baby formula recalled. A baby formula maker is recalling 3,030 cans of a specialty formula used for premature babies because they are contaminated with potentially life-threatening bacteria.** Recalled is a batch of EnfaCare LIPIL, a type of formula especially for preemies made by Mead Johnson Nutritionals. The recalled cans are embossed with the batch code BME01 and an expiration date of 1JAN04. **The batch is contaminated with a bacterium called *Enterobacter sakazaki*, which can cause meningitis, bloodstream infections, or a deadly intestinal inflammation in newborns, especially premature infants or others with weakened immune systems.** No illnesses have been reported, Mead Johnson said. U.S. Food and Drug Administration testing uncovered the contamination.

Source: http://www.11alive.com/news/news_article.asp?storyid=26172

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

Water Sector

14. *January 10, Woonsocket Call* — **Bacteria to tangle with toxic water.** It's called a biomass concentrator reactor. What the reactor is, is cutting edge technology that Rhode Island and federal environmental officials hope will make the cleanup of the water contamination in Pascoag a lot easier and cheaper. **Teaming up with the Rhode Island Department of Environmental Management (DEM), scientists with the Environmental Protection Agency (EPA) are expected to visit Pascoag this spring to test the bioreactor, which will use microorganisms, or bacteria, to clean up the petroleum-contaminated water.** Simply stated, a bioreactor is a piece of equipment that uses natural microbes to biologically treat groundwater flow, break down petroleum products and remove them from the environment. **More specifically, the bioreactor will use sphingomonas, a type of bacteria, to mineralize the methyl tertiary-butyl ether (MTBE) and other contaminants in Pascoag's groundwater.**

Source: <http://www.zwire.com/site/news.cfm?newsid=66588811fi=6>

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

Public Health Sector

Nothing to report.

Government Sector

15. *January 10, Washington Post* — Panel endorses new barriers for Washington Monument.

A federal design panel approved preliminary designs for security landscaping around the Washington Monument yesterday, but it stopped short of endorsing the National Park Service's sketches for a visitors' complex that would be partially underground. **The National Capital Planning Commission's endorsement of a series of pathways and low stone walls ringing the monument in concentric ovals is an attempt to protect the structure from bomb-carrying vehicles while preserving the aesthetic integrity of the area.** The landscaping plans, submitted by the Park Service, need final approval and funding. If that comes, the paths and walls -- which would be no more than 30 inches high -- would replace the rings of concrete Jersey barriers that now surround the monument.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A35597-2003Jan9.htm>

16. *January 10, New York Times* — Scientists discuss balance of research and security. The discussions at the National Academy of Sciences follow a raft of post-Sept. 11 restrictions on research into some 64 substances that could be used in biological weapons. The discussions were also partly an effort to fend off potential government censorship or other steps to control unclassified research that the new domestic security law terms "sensitive." **The talks were prompted by the hesitance of microbiologists to publish their full research in scientific journals out of concern that terrorists could use the information. While restrictions on research have long been a fact of life for chemists and nuclear physicists, they are new and not entirely welcome among microbiologists, who say data must be published so other scientists can verify the quality of the research by reproducing the results.** The discussions brought together two communities that have often viewed each other with distrust, if not disdain: security experts and scientists. **While some scientists contend that the best defense against biological weapons is robust research that is widely accessible, security specialists maintain that scientists are being naïve at best, and reckless at worst.**

Source: <http://www.nytimes.com/2003/01/10/science/10SECR.html>

Emergency Services Sector

17. *January 10, Federal Computer Week* — FBI expanding info-sharing test. Following a successful proof of concept demonstration of a law enforcement information-sharing project in St. Louis, the FBI is starting to test the initiative in more than seven cities across the country. **Although it is now funded as part of the agency's homeland security efforts, the Joint Terrorism Task Force Information Sharing Initiative began prior to Sept. 11, 2001, and is intended to help federal, state and local law enforcement work together on all kinds of criminal cases, said Bill Eubanks, manager of the initiative.** He was speaking Jan. 8 at the Government Convention on Emerging Technologies in Las Vegas. **By the end of the month, officials expect to have pilot projects running in St. Louis and San Diego.** In the next couple of months, further pilot projects will go live in Norfolk, Va., and Baltimore, working with the

Navy. And in May, the pilot project is expected to be ready in Seattle; Portland, Ore.; and Spokane, Wash., for a joint weapons of mass destruction exercise in the northwest.

Source: <http://www.fcw.com/fcw/articles/2003/0106/web-isi-01-10-03.asp>

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

Information and Telecommunications Sector

18. *January 13, Government Computer News* — **Commerce Department implementing IT security plan.** IT officials at the Commerce Department have implemented an IT security plan across the department that **includes guidance for developing system plans, for certifying and accrediting systems, and for handling IT security incidents both by detecting intrusions and responding to them.** The issue of systems security is receiving attention at high levels of the department, including the undersecretary, and **officials are ensuring that the department devotes resources to solving IT security problems,** Commerce CIO Tom Pyke said.

Source: http://www.gcn.com/22_1/it_infra/20791-1.html

19. *January 13, Government Computer News* — **Cyberwar may start with scholarships. A sustained digital attack on critical U.S. infrastructure wouldn't be easy to execute, but there are indications that some groups might be investing in the human resources such an attack would require,** said Matthew G. Devost, president of the Terrorism Research Center of Burke, Va. **Terrorist groups may be financing the education of computer science students to acquire the needed expertise,** he said, because "we're starting to see an increase in sponsorships of degrees." Devost spoke to law enforcement and intelligence officials today at a seminar sponsored by the Terrorism Research Center and the Washington Metro Transit Police. He said **terrorist organizations have shown a willingness to spend years in target selection and preparation for major attacks. Only now "are they in the process of capability acquisition" for cyberattacks,** he said, and **no students pursuing computer science degrees through sponsored scholarships have been tied to a particular organization.** Devost said his security consulting work has revealed an increase in insider attacks at companies by employees who appear to have sought their jobs specifically for that purpose. **So-called insider placement only becomes apparent when illegal or disruptive systems activity is noticed,** Devost said, and **a sleeper agent in a sensitive position probably could not be detected beforehand.**

Source: http://www.gcn.com/vol1_no1/daily-updates/20859-1.html

20. *January 10, International Data Group* — **Millions Lose Access to Microsoft Web Services.** An Internet routing error by AT&T shut off access from around 40 percent of the Internet to several major Microsoft Web sites and services on Thursday, Microsoft has said. **Access to Microsoft's Hotmail, Messenger, and Passport services as well as some other MSN services was cut for more than an hour. The changes were made in preparation for the addition of capacity between AT&T and Microsoft that is meant to improve access to the services hit by the outage,** said Adam Sohn, a spokesperson for Microsoft. **The problem is unrelated to an outage on Monday this week that left most of MSN Messenger's 75 million users unable to access the service for around five hours,** said Adam Sohn, a spokesperson for Microsoft. "We had not started the work with AT&T on Monday."

Source: <http://www.pcworld.com/news/article/0,aid,108662,00.asp>

21. *January 10, The Washington Times* — **Officials consider faster ways to alert U.S. to terrorism.** Sen. John Edwards, D–North Carolina, and Sen. Ernest F. Hollings, D–South Carolina, announced legislation to explore technology for new emergency alert systems yesterday. **The Emergency Alert System (EAS)** is used daily on the local level to issue warnings of events that can endanger the public. It is also used to transmit warnings from the AMBER (America's Missing Broadcast Emergency Response) alert system, which notifies the public about child abductions. **The EAS has never been used for its primary function, which is to provide the president with a means to address the nation through all broadcast, cable and satellite systems in the event of a national emergency.** It was not activated on September 11 because President Bush did not address the nation. The bill requires **the Commerce Department to develop new technologies to issue warnings based on the National Weather Service system, which is decoded by EAS equipment at broadcast and cable stations and can be delivered almost immediately.** Commerce would also explore **new ways to disseminate the warnings through the Internet, cell phones, and new technology to turn on TV sets.**

Source: <http://www.washtimes.com/national/20030110-90194169.htm>

22. *January 09, USA Today* — **Officials enlist hacker to foil piracy rings.** Federal prosecutors will tell a U.S. District Court in Tampa Friday of a plea deal with a hacker named Steven Woida. The deal includes his agreement to help them crack several international computer–chip–hacking groups. **By selling codes for smart cards – the devices that instruct set–top decoders to unscramble satellite TV signals – hackers have enabled as many as 3 million people to illegally watch DirecTV and EchoStar's Dish Network for free.** That amounts to an estimated \$4 billion a year in lost revenue for the industry. Woida, was arrested October 11 as he was making progress toward cracking the code for DirecTV's latest smart card, known as the P–4, they say. **He is believed to be one of just a few dozen people with the computer know–how and contacts to pull this off.** According to Customs' search warrant affidavit, Woida told them that **after the September 11 terror attacks "he received e–mails from unknown individuals in Afghanistan requesting that he perform hacking services for them."** He told Customs he didn't respond to the requests. Now, officials expect Woida to provide help **to foil attacks from Tunisia, Canada, Hong Kong and elsewhere on the USA's computer–based businesses.**

Source: http://www.usatoday.com/money/media/2003-01-09-satellite-pirate_x.htm

23. *January 08, Chronicle of Higher Education* — **West Point creates campus wireless network after overcoming security issues. The U.S. Military Academy, in West Point, N.Y., has begun using wireless networks in its classrooms.** But to secure the network, West Point had to pay about \$625,000, about five times what the network itself cost. **West Point officials say they had to invest in a much more secure approach because their campus network is connected to the Department of Defense (DOD) network, making it a more likely target of deliberate attackers.** "We cannot pose a threat to the rest of DOD through our network," says Colonel Donald J. Welch, associate dean for information and educational technology. In setting up their wireless network, WestPoint officials created a virtual private network (VPN), and installed 60 access controllers around the campus. **The software uses the federal government's most advanced encryption algorithm to guarantee the privacy of data files and network information.** The access controllers act as firewalls between the academy's

wireless-access hardware and the campus's wired network. **West Point is using a fast wireless technology, known as 802.11a, which requires more access devices than does the more commonly used but slower 802.11b technology.** The main advantage of the 802.11a networks, beside speed, Colonel Welch says, is that they are relatively free of the congestion that often disrupts communications on the slower networks. West Point's network is set up so that each classroom of eighteen or fewer students has its own wireless cell. Within that cell, the network bandwidth is about 25 megabits per second, or five times as fast as the effective bandwidth of 802.11b networks.

Source: <http://chronicle.com/free/2003/01/2003010801t.htm>

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), 21 (ftp), 445 (microsoft-ds), 3389 (ms-term-serv), 4662 (???), 53 (domain), 139 (netbios-ssn), 135 (???) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

24. *January 10, Reuters* — **Aid agencies can help respond to terror attacks.** Aid agencies could play a vital role in responding to a biochemical attack but governments must first share their expertise of weapons of mass destruction, the head of a medical charity said on Friday. With American and British troops preparing for war on Iraq and the discovery of small amounts of the deadly toxin ricin in a London flat, the threat of an attack with a biological or chemical agent looms larger than ever. **Geoff Prescott of the London-based medical charity Merlin said relief organizations should, but do not, have the capacity to deal with such disasters.** "This is a real issue of the 21st century and at the moment the only people who seem to be able to do anything about it are western militaries," he said in an interview. Merlin and the London School of Hygiene and Tropical Medicine have completed a study of the potential humanitarian response to such disasters and have called for a meeting with British officials in the hope of improving capabilities to deal with a biochemical attack. **"Our goal is to establish an**

independent, neutral humanitarian capacity to respond to casualties of weapons of mass destruction anywhere in the world and to gain that we will need to get help -- in the first stage only -- from western governments," he said.

Source: http://news.yahoo.com/news?tmpl=story2/20030110/sc_nm/health_attack_dc

25. January 10, Washington Post — Ex-clerk accused of DMV fraud. A former clerk in the Washington, D.C. Department of Motor Vehicles was charged yesterday with taking part in a scheme to sell hundreds of fraudulent driver's licenses to immigrants mostly from the Middle East, south Asia and Russia. **The charges, contained in a federal grand jury indictment in New York, accuse the clerk, Gwendolynn Dean, 48, of Washington, along with Rafet Ozoglu, 41, of Brooklyn and Mustafa Ozsusamlar, 58, of Manhattan, with conspiring to sell fraudulent driver's licenses to immigrants for about \$1,500 a piece. The indictment accuses the three of a scheme involving more than 900 such licenses, a number considerably higher than investigators initially thought.** In October, the three were charged with selling about 100 fraudulent licenses.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A35890-2003Jan9.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.