



National Infrastructure Protection Center NIPC Daily Open Source Report for 16 January 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports the Nuclear Regulatory Commission is changing the way it regulates the nation's nuclear power plants and will create a mechanism for faster intervention when irregularities are spotted. (See item [3](#))
- The General Accounting Office has published a report entitled "Vulnerabilities and Potential Improvements for the Air Cargo System" on the security vulnerabilities that have been identified in the air cargo system. (See item [11](#))
- The Knoxville News Sentinel reports Oak Ridge National Laboratory researchers have installed about 20 sensor packages around Washington, D.C., as one of the first tests of the SensorNet system designed to combat chemical and radiological terrorism. (See item [25](#))
- CERT announces Vulnerability Note VU#284857: Buffer overflows in ISC DHCPD minires library, which is used by NSUPDATE to resolve hostnames. (See item [26](#))
- The Wall Street Journal reports Federal agents are investigating whether Chinese companies were involved in alleged attempts to steal vital commercial technologies from two Silicon Valley companies in an emerging pattern of trade-secrets thefts. (See item [33](#))

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 15, Business Day* — **Russia urged to stabilize world oil markets. Russia can play a**

leading role in stabilizing global oil markets as prices continue to surge amid fears of war in Iraq and a strike in Venezuela, OPEC secretary-general Alvaro Silva-Calderon said in an interview published on Wednesday. "Russia can now play an extremely important role," Silva-Calderon told the Vremya Novostei daily, while urging closer co-operation between Russia and the oil cartel. Russia, one of the world's top oil exporters but not a member of the Organisation of Petroleum Exporting Countries (OPEC), earlier this month pledged full co-operation with OPEC to boost deliveries and stem the steady rise in world prices. **Russia can play a leading role in stabilising global oil markets as prices continue to surge amid fears of war in Iraq and a strike in Venezuela, OPEC secretary-general Alvaro Silva-Calderon said in an interview published on Wednesday. Oil prices surged Tuesday, with New York's light sweet crude for February delivery rising 11 cents higher to \$32.37 a barrel. The surge in prices wiped out any brief respite for oil consumers provided by OPEC's decision in Vienna on Sunday to raise its output quota by 1.5 million barrels a day from February.**
Source: <http://www.bday.co.za/bday/content/direct/1.3523.1263565-6078-0.0.0.html>

2. *January 15, Associated Press* — **Study reports California energy crisis costs \$45B . California's energy crisis cost the state as much as \$45 billion over two years in higher electricity costs, lost business due to blackouts and a slowdown in economic growth, according to a study released Wednesday. The report, from the Public Policy Institute of California, concluded there was no one cause for the energy crisis, which peaked in the winter of 2000-01 and led to six days of rolling blackouts. A shortage of electricity generating capacity, a flawed market design from the state's attempt at deregulation, the grip energy companies had over wholesale electricity prices and regulatory missteps all contributed to the energy crisis that spread to other Western states. But the state was also hit by circumstances it couldn't control. In 2000, the cost of natural gas and air quality credits rose, making electricity production more costly, and a drought in the Northwest limited the supply of electricity from hydroelectric sources. "Even if the electricity sector had remained regulated, prices would have increased, and some blackouts would have possibly occurred between May 2000 and June 2001," said the report, which was written by Christopher Weare, a research fellow at the institute. Retail rate increases by the California Public Utilities Commission helped utilities stave off more debt and encouraged conservation. And the Federal Energy Regulatory Commission's wholesale price cap in June 2001 limited how much generators and marketers could charge helped stabilize the market.**
Source: <http://www.washingtonpost.com/wp-dyn/articles/A58060-2003Jan15.ht ml>
3. *January 14, Associated Press* — **NRC to change the way it regulates.** The Nuclear Regulatory Commission (NRC) is overhauling the way it regulates the nation's nuclear power plants in response to criticism that it should have detected damage to an Ohio nuclear reactor sooner. **The commission on Tuesday adopted nearly all 50 staff recommendations from a highly critical report on the Davis-Besse plant in Oak Harbor which is near Toledo, OH. Those recommendations include conducting more thorough inspections; demanding better assurances from plant operators that problems get fixed; and creating a mechanism for faster intervention when irregularities are spotted. The changes come 10 months after inspectors found boric acid had nearly eaten through a 6-inch-thick steel reactor cap on the Davis-Besse plant.** The discovery, which the NRC has said should have been spotted several years earlier, led to a nationwide review of all 69 similar plants. "We're trying to set tripwires out there so when someone sees a problem they can bring it to the

attention of management," said Carl Paperiello, NRC's deputy executive director for materials, research and state programs. Paperiello chaired the review team that approved the reforms. The time frame for the reforms to be implemented ranges from six months to two years. The NRC will file a status report every six months to make sure the reforms are carried out.

Source: <http://www.wjla.com/news/stories/0103/69697.html>

4. *January 14, Chicago Tribune* — **Russia shuts down infamous site of nuclear disaster. . . Russia has shut down a notorious, aging nuclear plant responsible for decades of environmental ruin in the Ural Mountains, a decision heralded Monday as an unexpected shift in how Moscow views dangers posed by nuclear waste. The plant in Mayak, in central Russia, had been dumping radioactive waste into a nearby lake, contaminating drinking water for thousands of people. More than 40,000 Russians living in the villages and hamlets surrounding Mayak have been treated for the effects of radiation exposure in the last 10 years.** Officials with Gosatomnadzor, Russia's nuclear safety agency, said Monday that they denied the plant a license to continue operations this year because of evidence that it was contaminating local drinking water. "We are now deciding on what conditions need to be fulfilled so that work can resume," said Andrei Kislov, a senior official at Gosatomnadzor. **Known as Plant 235, the facility is part of a large complex that includes a U.S.–Russian project to store plutonium from Russia's dismantled nuclear weapons. The plant was the site of one of the former Soviet Union's worst nuclear accidents, eclipsed only by the 1986 disaster at Chernobyl in what is now Ukraine. In 1957 a radioactive waste tank at Mayak exploded and exposed more than 470,000 people to radiation. Officials kept the accident secret for years. Since 1979, spent fuel from Russian nuclear power plants and nuclear submarines has been shipped to Plant 235, where reactor–grade plutonium was extracted for reuse. The recycling regimen produced radioactive waste that the plant dumped into Lake Karachay and the nearby Techa River. Plant officials have said they lacked the technology to dispose of the waste any other way,** said Vladimir Sliviyak, co–chairman of Ecodefense, a Russian environmental group. "We are very happy that the reprocessing of radioactive waste at Mayak is going to be suspended," Sliviyak said. "This is what we demanded a long time ago. The region has been suffering because of this plant for the last 50 years." Sliviyak said the Plant 235 decision stops plutonium extraction at the facility.

Source: http://www.energycentral.com/sections/newsroom/nr_article.cfm?id=3569597

5. *January 14, Associated Press* — **Nuke plant security readiness scrutinized. The head of the county that is home to the Indian Point nuclear plant said Monday he will withhold approval for the facility's evacuation plans until the federal government addresses a study warning the plant is unprepared for terrorist threats.** Westchester County Executive Andrew Spano said the study, which was commissioned by Gov. George Pataki and released Friday, shows guidance from Washington is needed to ensure security. He threatened to call for the shutdown of the plant if such help does not come. After the report's release, Pataki did not call for a shutdown, as some activists had hoped, but called on FEMA and the Nuclear Regulatory Commission to "look at the standards used to certify these emergency plans and determine if they are strong enough to meet the post–Sept. 11 reality." **An estimated 11.8 million people live within 50 miles of Indian Point, far more than around any of the nation's other nuclear plants.**

Source: http://www.energycentral.com/sections/newsroom/nr_article.cfm?id=3569817

6. *January 13, USA Today* — **Natural gas prices rise as temps fall. Natural gas prices are climbing quickly. Futures prices for natural gas are up more than 130% from last year and are the highest since April 2001. The gain not only is squeezing budgets for the 55% of U.S. homeowners who use natural gas to heat their homes, it's also bad news for the economy. As consumers spend more money on energy, they have less cash to spend in other areas, such as department stores or beauty shops, that need a boost.** Relief from the higher costs is nowhere in sight. "We see continued pressure on natural gas prices for the next one to two months," Guy Caruso, head of the Energy Information Administration, a division of the Energy Department, told reporters last week. Prices are also up for other forms of energy. **The EIA estimates winter heating bills will be up 43% for heating oil customers, 20% for propane and 12% for electricity this year. Despite the gain, prices are not expected to come close to winter 2000–01, when costs rose to the highest in more than a decade.**
Source: http://www.usatoday.com/money/markets/us/2003-01-13-natgas_x.htm

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

7. *January 15, Government Computer News* — **Joint Chiefs will focus on data-sharing initiative.** The Joint Chiefs of Staff is spearheading work on a strategy for how the military branches share information, secure command and control assets, and fight future wars. "If our military is to defeat our adversaries, we must improve how we share information," Air Force Gen. Richard B. Myers, head of the Joint Chiefs, said. "Information sharing allows transparency in both planning and execution. History is pretty clear. The one who can do that the fastest, usually wins." **The operational Joint Capstone Document will come from the perspective of the warfighter and will exploit what Myers called "our nation's asymmetrical advantages."** **The Joint Chiefs is working with the individual services, think tanks, universities and technology vendors to create the document, Myers said.** "We are putting a lot of energy behind better solutions," he said. "Transformation must be more than a bumper sticker. Transformation isn't just about words; it's about results." **Myers gave the keynote address on tuesday at the Armed Forces Communications and Electronics Association's West 2003 conference in San Diego. He spoke via telecast from the Pentagon.**

Source: http://www.gcn.com/vol1_no1/daily-updates/20871-1.html

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

Banking and Finance Sector

8. *January 15, Associated Press* — **China details regulations against money laundering.** China has outlined its first regulations that target money laundering, saying it will order banks and

other financial institutions to take responsibility for suspicious transactions it says are threatening the economy. **Outlining specifics of regulations announced earlier in the week, the People's Bank of China, or central bank, ordered banks on Wednesday to verify the identities of accountholders and keep records of large or suspicious dealings for at least five years.** China pledged last summer to take action against money laundering, partly to stanch the 200 billion yuan (US\$24.2 billion) reportedly flowing illegally out of the country each year through underground banks and other illicit channels. **Regulators fear growing illegal transactions threaten the country's financial stability. Money laundering enables corrupt officials and tax evaders to hide ill-gotten gains and often sneak them out of the country, sapping national coffers, said the English-language newspaper China Daily.**

Source: http://story.news.yahoo.com/news?tmpl=storyp_woen_po/as_fin_china_money_laundering_1

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

Transportation Sector

9. *January 15, U.S. Department of Transportation* — **Transportation Secretary Mineta announces \$54M in 9/11 funding for ferry facilities in New York and New Jersey.** U.S. Secretary of Transportation Norman Y. Mineta announced Wednesday that the **Federal Transit Administration (FTA) will provide approximately \$54.8 million for ferry-related projects in the New York City-Northern New Jersey metropolitan area to support the expansion of interstate ferry services due to the loss of Port Authority Trans-Hudson (PATH) train service between New Jersey and Lower Manhattan on September 11, 2001.** This funding for ferry-related projects supplements \$100 million that was previously approved by FTA and distributed to the region for emergency transit capital improvements, and is a part of President Bush's \$20 billion commitment to rebuild and revitalize Lower Manhattan.
Source: <http://www.dot.gov/affairs/fta0203.htm>

10. *January 14, Associated Press* — **Bush Designates Leader for Safety Board.** President Bush said Tuesday he would elevate Republican John Hammerschmidt to vice chairman of the **National Transportation Safety Board, enabling him to take over when the acting chairman's term expires this weekend.** The move means Hammerschmidt will become acting chairman on Saturday, replacing Carol Carmody.
Source: <http://www.washingtonpost.com/wp-dyn/articles/A56343-2003Jan14.htm>

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

Postal and Shipping Sector

11. *January 15, General Accounting Office* — **Aviation security: vulnerabilities and potential improvements for the air cargo system.** The General Accounting Office (GAO) has released its December 2002 report to Congress on Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. GAO agreed to determine the security vulnerabilities that have been identified in the air cargo system, the status of key recommendations that have been made since 1990 to improve air cargo security, and ways in which air cargo security can

be improved in the near- and long-term. Numerous government and industry studies have identified vulnerabilities in the air cargo system. **These vulnerabilities occur in the security procedures of some air carriers and freight forwarders and in possible tampering with freight at various handoffs that occur from the point when cargo leaves a shipper to the point when it is loaded onto an aircraft. As a result, any weaknesses in this program could create security risks.** Federal reports, industry groups, and security experts have identified operational and technological measures that have the potential to improved air cargo security in the near term. Each potential improvement measure, however needs to be weighed against other issues, such as costs and the effects on the flow of cargo. **Therefore, the GAO recommends that the Transportation Security Administration develop a comprehensive plan for air cargo security that identifies priority actions on the basis of risk, costs, and performance targets, and establishes deadlines for completing those actions.**

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-03-344>

12. *January 15, Federal Computer Week* — **Customs writing cargo data rules. The Customs Service has begun the task of writing regulations requiring that the electronic manifest for each air cargo shipment be sent to a government database before the shipment leaves a foreign port for the United States. New rules are expected to go into effect Oct. 1 for air, rail, sea and truck cargo in a move to tighten border security, but first Customs faces the problem of figuring out how to handle the data electronically without stalling the flow of commerce.** Customs, which officially becomes part of the Homeland Security Department Jan. 24, is holding four days of hearings to get feedback from industry on how to comply with the Maritime Transportation Security Act of 2002. But at the first hearing on Jan. 14, industry participants made it clear that requiring a 24-hour notice before liftoff and risking delivery delays could hurt airline shipping. Customs officials readily acknowledged it is a tough problem for them. **They are in the process of building a Web-based data system called the Automated Commercial Environment (ACE). The system is intended to provide electronic information about cargo inspections and clearance into the United States, but it will not be fully operational until 2007.** In the meantime, Customs must still rely on the aging Automated Commercial System to handle the manifest data.

Source: <http://www.fcw.com/fcw/articles/2003/0113/web-customs-01-15-03.as.p>

13. *January 15, Washington Post* — **Northeast Washington, DC mail facility closed after possible anthrax finding. A Postal Service facility for sorting U.S. government mail in Northeast Washington was shut last night as a precaution after a letter sent to the Federal Reserve Board showed the possible presence of anthrax spores, officials said.** In halting operations at the facility in the 3300 block of "V" Street, the Postal Service appeared to be going beyond previous responses to the discovery of possible anthrax contamination of government mail. Thomas G. Day, the Postal Service's vice president of engineering, said the move was made "out of an abundance of caution. There is no evidence that there is any contamination at the facility," Day said, adding that there also was "no evidence that any employee or member of the public has been exposed to any health risk." Mail sorted on "V" Street goes to the Fed and other government destinations. Tests showing that the letter was possibly contaminated were made by the Fed at its own mail-sorting facility, Fed spokeswoman Michelle Smith said. She said tests at an outside laboratory gave the same findings. Further testing is to be conducted at the Centers for Disease Control and Prevention in Atlanta.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A57071-2003Jan14.html>

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

Agriculture Sector

14. *January 15, Statesman Journal* — **Oregon delivers bass for virus research. About 50 largemouth bass from Oregon have become transcontinental organ donors. The fish are providing tissue for research to help discover the causes and mechanisms of a disease known as largemouth bass virus.** The virus is endemic in many lakes in the South and has caused several fish kills, the largest a 5,000 largemouth dieoff in 1999 at Lake Fork, TX. One hitch for biologists is it's difficult to find bass that have not been exposed to the virus, said John Grizzle, a research professor at Auburn University's Department of Fisheries and Allied Aquacultures in Auburn, Al. "In the Southeast, it appears to be very widespread. We had a hard time coming up with populations without the virus," he said. "You kind of have to assume they're positive until proven otherwise." "Originally, the conservation director (for the Bass Anglers Sportsmans Society) in Alabama called me," said Chuck Lang of Salem, the society's conservation director for Oregon. "He said Dr. Grizzle was looking for a place where there, hopefully, was no largemouth bass virus." Grizzle told Lang that 60 largemouth bass, 12 inches or longer, frozen alive, were needed to help the study. **The Oregon bass eventually could help solve the largemouth bass virus puzzle, Grizzle said.**

Source: <http://news.statesmanjournal.com/article.cfm?i=54934>

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

Food Sector

Nothing to report.

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

Water Sector

15. *January 15, Orlando Sentinel* — **Local officials are criticizing the way a break-in at the local water plant in Volusia County was handled, an incident that resulted in the shutting off of water services to many residents in the region. According to the Orlando Sentinel, roughly 30 hours passed between the discovery of the break-in Sunday morning and Monday's precautionary shutdown of the water plant, which serves more than 4,000 customers in southwest Volusia. The security breach prompted hours of bureaucratic debate before residents were alerted to the possible danger, the newspaper said, but the emergency-notification system failed to reach thousands of residents with the final decision: Don't drink, bathe or cook with the water.** Dave Byron, a county spokesman, said Tuesday that county officials believed there was no access to the water system during the break-in, the article said. Byron said county officials disagreed with the Health Department's assessment of the situation but made efforts to notify residents as quickly as possible, the newspaper said.

Source: <http://www.watertechonline.com/news.asp?mode=4font>

Public Health Sector

16. *January 15, BBC News* — **DNA databases 'no use to terrorists'. Some have raised the possibility that terrorists could take publicly available data on harmful microbes and use new genetic engineering techniques to turn the information into lethal bio-weapons.** This prospect has led to calls for the classification of the genome data of harmful organisms. A leading scientist in the field has told BBC News Online that potential bioterrorists would not be able to manufacture genetically modified killer viruses or bacteria using the databases. Genome pioneer Dr. Claire Fraser, of The Institute for Genomic Research (Tigr), says that although the genetic data of human pathogens is public, no one knows enough to turn this information into bioweapons. **The U.S. National Academies and the Center for Strategic and International Studies has held a conference to discuss the so-called weaponisation of genomes.** As well as Dr. Fraser, on the panel was George Poste, chair of the U.S. Department of Defense Task Force against Bioterrorism. **Poste described tailor-made microbes that produce powerful toxins, evade antibiotics, and even produce "stealth viral vectors" that can integrate pathogenic DNA directly into an individual's genome.** Although scientists have a lot of genetic information about bacteria and viruses that could, in principle, be used to generate superbugs, Dr. Fraser said there was so much we did not understand about gene function that such information would be of no practical use to a bioterrorist.

Source: <http://news.bbc.co.uk/1/hi/sci/tech/2660753.stm>

17. *January 15, Reuters* — **CDC advisors discuss smallpox vaccine details. As the rollout of the smallpox vaccine for 500,000 healthcare workers approaches, experts advising the U.S. Centers for Disease Control and Prevention (CDC) updated recommendations about who should receive the vaccine. On Thursday, the CDC's Advisory Committee on Immunization Practices (ACIP) noted that in very rare cases, vaccinated individuals have been known to spread the vaccine virus to babies under 1 year old.** While the group still recommends that healthcare workers with a baby in their household be vaccinated, the ACIP said that some states may want to defer vaccination of such individuals. Smallpox vaccines are not routinely given to young infants, due to the potential risk of vaccinia-related side effects. People who have autoimmune diseases or are taking medications for such illnesses should not receive the smallpox vaccine. The committee agreed to add to the statement language that further clarifies these conditions to aid physicians advising patients about getting the vaccine. **In addition, the ACIP will recommend that people with any inflammatory disease of the eye or recent ophthalmic surgery requiring steroid therapy wait until the treatment is complete to receive the smallpox vaccine.**

Source: <http://reuters.com/newsArticle.jhtml?type=healthNews207>

18. *January 15, Reuters* — **EU studies threat of biological attack.** In an interview with Reuters, Stefan Kaufmann, one of the European Commission's 14-member Expert Group on Countering the Effects of Biological and Chemical Terrorism, said the danger was small but real. "There is a low risk, but if something happens, the consequences will be enormous," he said. "Politicians have to do something because we cannot say that it is a zero chance." **Kaufmann, an immunologist and head of Berlin's Max Planck Institute for Infection Biology, said the**

European Commission was better placed to oversee plans for responding to biological threats than individual EU states, but had little funding. The confidential report completed by the Commission's expert team late last year outlines a number of scenarios involving deliberate releases of biological and chemical agents. **The group assessed potential weak points such as the food chain, water supply, or health systems which could be at risk.** Kaufmann said scientists still do not fully understand many of the germs which could be used in an attack, but the EU's preparedness had improved since a German anthrax scare in 2002.

Source: <http://www.alertnet.org/thenews/newsdesk/L15093027>

19. *January 15, Kingsport Times–News* — **Tennessee has among highest levels of antibiotic resistance in country. In doctors' offices and hospitals throughout Tennessee, antibiotics are often seen as a quick–fix solution for patients, which has resulted in this state having one of the highest levels of antibiotic resistance in the country, according to the Department of Health in Nashville.** The Tennessee Department of Health joined other organizations in May 2002 to spread the word that antibiotics won't help if you have a cold or the flu and that, unless inappropriate antibiotic use is curbed, bacteria will eventually become immune to the strongest drugs. Tennessee's Appropriate Antibiotic Use Campaign seeks to reduce inappropriate antibiotic use and the spread of antibiotic–resistant bacteria, which are an increasing proportion of the number of bacterial infections. **"In some areas of Tennessee, people can no longer use penicillin to treat ear infections, pneumonia and other serious infections because the bacteria causing the illness is stronger than the antibiotic," said Allen Craig, state epidemiologist.** "When this occurs, practitioners must use stronger and sometimes more expensive antibiotics to cure common infection." **"Unless we begin to curb the inappropriate use of antibiotics, bacteria will eventually become impervious to even the strongest drugs. If that happens, antibiotics will become less and less effective and it will become more difficult to treat common bacterial infections,"** he said.

Source: <http://www.timesnews.net/article.dna? StoryID=3167417>

20. *January 14, Knight Ridder Newspapers* — **Hospitals, blood banks grapple with critical blood shortage. Hospitals and community blood banks across the nation are experiencing a blood shortage so severe that some are postponing non–emergency surgeries and thawing frozen blood, a measure that makes it more perishable. "Some hospitals have only a one–day supply. About 50 percent have less than two days,"** said Brooke Thaler, spokesperson for America's Blood Center, a coalition of U.S. blood centers based in Washington, D.C. Blood centers like to have at least a seven–day supply on hand, Thaler said. The American Red Cross, which supplies about half the nation's blood needs, says two–thirds of its blood donation centers nationwide have issued emergency appeals. **If the U.S. invades Iraq, the demand for blood will put further pressure on supplies. During the last conflict with Iraq, 20 percent of the blood shipped to the troops came from civilian blood banks.** "We don't have any blood available on our shelves at all," said Robin Davidson, spokeswoman for the Gulf Coast Regional Blood Center in Houston, Texas, where the situation is especially critical. The blood bank, which serves 24 counties and 220 hospitals or health care centers, has hundreds of unfulfilled requests for blood, she said. The Gulf Coast Regional Blood Center has resorted to thawing frozen stocks of blood, Davidson said, because "If there is a crisis like there is now, you can't thaw it fast enough." The process is time–consuming, in part because it requires the removal of additives. Once thawed, the blood is good for less than 24 hours.

Unfrozen red blood cells are good for 42 days.

Source: <http://www.kansas.com/mld/kansas/news/4946472.htm>

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

Government Sector

21. *January 15, Washington Post* — **Homeland security staff moves slowed.** Homeland security secretary–nominee Tom Ridge will not move from temporary offices in downtown Washington, D.C. to new department headquarters in Northern Virginia until spring, aides said. While the headquarters site is to be selected from a handful of contenders as early as today, **government officials said, only about 2,200 federal employees will work in the new facility by year's end. That level is likely to be maintained for the foreseeable future and is more comparable to a medium–size corporate headquarters than a sprawling complex such as the Pentagon.** The staffing estimates, cited in leasing papers and budget data submitted to Congress, indicate that contrary to some expectations on Capitol Hill and elsewhere, the new Department of Homeland Security headquarters will not create a giant new government installation in Virginia, at least not right away. **About 177,000 workers from 22 agencies are being consolidated into the department nationwide.** The plan also raises the possibility of a future round in the fight among Virginia, Maryland and the District to permanently host the agency. If all 17,000 workers moved into one facility, they would require 4 million square feet of space, real estate executives said.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A57354-2003Jan14.ht ml>

22. *January 15, Middle East Newsline* — **U.S. begins pullout of non–essential staff from Mideast.** The United States has launched an effort to withdraw non–essential government personnel from the Middle East. Officials said the effort is meant to avoid Arab or Islamic reprisals on U.S. personnel over the next few months amid tension in the Persian Gulf and Middle East region. They said U.S. intelligence agencies have warned that Al Qaida and Iraq could intensify attacks on U.S. nationals to foil any Washington–led war against Baghdad. **So far, officials said, the State Department is quietly pulling out non–essential embassy staffers and families in such countries as Egypt, Jordan, Kuwait, Lebanon, Morocco and Saudi Arabia. They said similar measures will be taken in the United Arab Emirates and other countries.**

Source: http://www.menewsline.com/stories/2003/january/01_15_1.html

23. *January 15, Law.com* — **DEA employee gets prison term for leaking info to reporter.** A federal judge in Atlanta has imposed a one–year prison sentence on a former Atlanta Drug Enforcement Administration (DEA) analyst charged with stealing government information and leaking it to a London newspaper. **In a case that the U.S. Attorney in Atlanta says establishes a significant precedent, federal prosecutors assigned a media market price to the leaked information high enough to ensure a felony charge and increase the anticipated prison term.** William S. Duffey Jr., U.S. Attorney for the Northern District of Georgia, said the successful prosecution of former Atlanta DEA analyst Jonathan Randel stands as a warning to government employees, particularly law enforcement agents, who might consider providing sensitive, unclassified information to anyone, including journalists, outside of the federal government. "It is our intention to prosecute those offenses," Duffey said. "We have to send

that message to everybody within the justice system." **Duffey's prosecution of Randel is in line with a report by U.S. Attorney General John Ashcroft's interagency, anti-leak task force, which last year recommended that government administrators use laws already on the books to identify and punish employees who leak information.**

Source: http://biz.yahoo.com/law/030115/043a320e7cb358643dc2b77dba01e27d_1.html

24. *January 15, Federal Computer Week* — **Intell info sharing makes strides.** The sharing of intelligence information, at least in the unclassified arena, recently has taken several significant steps forward through a newly minted partnership among segments of federal, state and local governments. **From September to December 2002, officials completed at least the initial integration of collaboration networks from the FBI, local law enforcement, the intelligence community and the State Department, allowing functions ranging from secure e-mail exchange to searches of one another's databases.** Work remains to be done on those systems, and others are in the pipeline for connection, but analysts and operational employees are already seeing a difference, officials said at the Government Convention on Emerging Technologies in Las Vegas. "We have the opportunity to make the most significant impact on law enforcement in decades, just by getting us on one network," said Craig Sorum, chief of the Law Enforcement Online (LEO) unit at FBI headquarters. **The intelligence community's Open Source Information System (OSIS) now serves as a central hub connecting State's intranet, called OpenNet, and the FBI's LEO. State and local law enforcement officials can access those federal resources thanks to the recent integration of LEO and the Justice Department's Regional Information Sharing System (RISS) Program, which is composed of six regional centers that share intelligence and coordinate against criminal efforts.** The new connections allow additional civilian agencies to access the OSIS homeland security portal, where the intelligence community has centralized all the open-source information it has gathered in that area, said John Brantley, director of the Intelink Management Office, which runs OSIS. In addition to providing new information to new partners, the network allows collaboration "that simply didn't exist before," he said.

Source: <http://www.fcw.com/geb/articles/2003/0113/web-info-01-15-03.asp>

[[Return to top](#)]

Emergency Services Sector

25. *January 15, Knoxville News Sentinel* — **ORNL installs anti-terror sensors in Washington.** Oak Ridge National Laboratory researchers have installed about 20 sensor packages in Washington, D.C., as one of the first tests of the SensorNet system to combat terrorism. **The chemical and radiological sensors are being tested in conjunction with meteorological equipment installed earlier by the National Oceanic and Atmospheric Administration. Biological detectors are not part of the Washington test but will be included in future operations. Dick Reid of ORNL declined to specify the location of sensors in the nation's capital, but he said they are positioned on rooftops, at street level and on cell-phone towers. Workers began installing the sensors in November, he said.** ORNL researchers will use chemical simulants to test the effectiveness of detectors, as well as the communications network. The Washington system will remain activated to provide alerts in case of an actual release of hazardous materials. "It's a pilot system, but it's also a leave-behind," Reid said. "When we're finished testing, we'll leave the sensors behind." Reid said workers are setting up a

SensorNet command center at the National Transportation Research Center in Knoxville, where information from a variety of test sites will be received and evaluated. The command center could be operable by the end of January, he said. **ORNL has proposed SensorNet as an early-detection system for terrorist attacks involving chemical, biological and radioactive agents. The system of modular detectors is designed for deployment on cell-phone towers around the country, using wireless and satellite communications to relay data quickly to first responders. The goal is to have information to responders within five minutes of detection. Last year, the lab successfully demonstrated the capabilities with tests in Knoxville, Nashville and Chattanooga.**

Source: <http://www.csm.ornl.gov/PR/NS01-10-03.html>

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

Information and Telecommunications Sector

26. *January 16, CERT/CC* — VU#284857: Buffer overflows in ISC DHCPD minires library.

During an internal source code audit, developers from the Internet Software Consortium (ISC) discovered **several vulnerabilities in the error handling routines of the minires library, which is used by NSUPDATE to resolve hostnames.** These vulnerabilities are **stack-based buffer overflows that may be exploitable by sending a DHCP message containing a large hostname value.** Note: Although the minires library is derived from the BIND 8 resolver library, these vulnerabilities do not affect any current versions of BIND. At this time, CERT is not aware of any exploits. The ISC has addressed these vulnerabilities in versions 3.0p12 and 3.0.1RC11 of ISC DHCPD. More information may be found on the ISC Website:

<http://www.isc.org/>

Source: <http://www.cert.org/advisories/CA-2003-01.html>

27. *January 15, New York Times* — Microsoft to give governments access to code. Microsoft announced today that it will allow most governments to study the programming code of its Windows systems. Under the program, **97 percent of the code to Windows desktop, Windows server and Windows CE hand-held software will be available to governments online for inspection and testing.** To view the other 3 percent – the most sensitive technology – government representatives must come to Microsoft headquarters in Redmond, WA. **Governments will also be allowed to plug their security features instead of Microsoft's technology into Windows.** More than two dozen countries are encouraging agencies to use "open source" software – developed by programmers who distribute the code without charge and donate their labor to debug and modify the software cooperatively. The best-known of the open source projects is GNU Linux, an operating system that Microsoft regards as the leading competitive threat to Windows. **One appeal of Linux is that developers have complete access to the underlying source code, whereas Microsoft has kept some Windows technology secret. Microsoft expects that perhaps 60 foreign governments and international agencies will eventually join its government security program.** The first to join were Russia and the North Atlantic Treaty Organization, and the company is negotiating with 20 other groups.

Source: <http://www.nytimes.com/2003/01/15/technology/15SOFT.html>

28.

January 15, New York Times — FCC chief dismisses talk of extensive rule changes. Michael K. Powell, the chairman of the Federal Communications Commission (FCC), reassured Congress today that there would not be radical changes in rules governing local phone service, high-speed Internet access and ownership of media outlets, but Democratic and Republican senators said they were worried that anticipated changes could hurt consumers. The combination of technological changes and company failures, including the collapse of WorldCom, as well as judicial rejection of some commission rules have added to the importance of coming federal rule changes. **A crucial area being reviewed is the federal limit on concentrated ownership of television stations and newspapers. Other rules specify that a broadcaster may not own television stations that broadcast to more than 35 percent of the nation's homes, and a broadcaster may not own two television stations in the same market unless there are at least eight other competitors.** Powell acknowledged that he was concerned about growing concentration in radio station ownership, where a few large companies bought up many local stations after Congress relaxed the rules in the Telecommunications Act of 1996. Powell said that the way the agency calculated ownership levels in local markets could be adjusted, and noted that media company mergers and acquisitions are still subject to approval by regulators.

Source: <http://www.nytimes.com/2003/01/15/technology/15PHON.html>

29. *January 13, Security Focus* — **Federal government to seek public input on hacker sentencing.** Last week the presidential-appointed commission responsible for setting federal sentencing rules **formally asked the public's advice on the formula used to sentence hackers and virus writers to prison or probation.** The **United States Sentencing Commission's (USSC) Federal Sentencing Guidelines set the range of sentences a court can choose from in a given case, based on a point system** that sets a starting value for a particular crime, and then adds or subtracts points for specific aggravating or mitigating circumstances. **Though they're called "guidelines," the rules are generally binding on judges.** Computer crimes currently share sentencing guidelines with larceny, embezzlement and theft, where the most significant sentencing factor is the amount of financial loss inflicted. But in a congressional session that heard much talk about "cyberterrorism," lawmakers became convinced that computer outlaws were more than common thieves. Consequently, **one of the provisions in the Homeland Security Act passed last November requires the USSC to review the cyber crime sentencing guidelines to ensure they take into account "the serious nature of such offenses, the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses."** The USSC's "Issue for Comment" is available on the Commission's Website: <http://www.ussc.gov/>. **The public comment period ends on February 18th.**

Source: <http://online.securityfocus.com/news/2028>

30. *January 13, eWeek* — **Sharing attack data could thwart hackers.** Two Harvard University security researchers have developed **a model showing that enterprises that share their sensitive data about network attacks and security breaches are less attractive targets and, hence, less likely to be attacked.** The reason is that attackers who spend time, and in some cases money, **finding and exploiting vulnerabilities in common applications will not want information about their attacks shared, as it would reduce their chances of compromising other potential targets.** The paper, to be presented later this month at the Financial Cryptography conference in Gosier, Guadeloupe, supports the U.S. government's contentions

about the importance of sharing attack data. The next draft of the **National Strategy to Secure Cyberspace, due early this year, is expected to include language encouraging CIOs to forward more information to the government.** Security specialists and CIOs worry that sharing sensitive data with anyone will expose them to embarrassment and potential lawsuits from customers. **The government's interest in attack data is partially due to the creation of the Department of Homeland Security which will be responsible for early warning and analysis.**

Source: <http://www.eweek.com/article2/0.3959.825430.00.asp>

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: PE_FUNLOVE.4099 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), 53 (domain), 4662 (???), 139 (netbios–ssn), 135 (???), 27374 (asp), 443 (https) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

31. *January 15, USA Today* — **Suspect helping U.S. gauge al Qaeda's arsenal.** Alleged al Qaeda operative Ramzi Bin al–Shibh is providing U.S. intelligence officials with valuable information about the terrorist group's potential for using nuclear, biological and chemical weapons, according to U.S. government sources. **The interrogation of Bin al–Shibh has been "very productive in understanding what the capability was, how close to nuke–bio–chem they were" up to the time of the Yemeni cleric's capture in Pakistan in September, one source says. Bin al–Shibh, one of a handful of living suspects in the Sept. 11 conspiracy, also is revealing helpful details about al Qaeda's command structure, the sources says.** Since his capture, Bin al–Shibh, 30, has expressed "zero remorse," one source says. "He's made it clear that had he not been captured, he would've continued doing what he had been doing." The sources will not elaborate on information provided by Bin al–Shibh, who allegedly wired money from Europe to Zacarias Moussaoui, the only person charged in the U.S. in the September 11 conspiracy. **But officials believe Bin al–Shibh's revelations about weapons of**

mass destruction and al Qaeda's command structure will be important to the CIA, FBI and Defense Department for "some time to come," one source says.

Source: http://www.usatoday.com/news/washington/2003-01-14-investigate-us_at_x.htm

32. *January 15, New York Times* — **Terror arrests in England. A police officer was stabbed to death and four others were wounded tuesday night during the arrests of three terror suspects in Manchester that the police said were linked to the discovery last week of the deadly poison ricin in London.** The 40-year-old officer, whose name was withheld, was attacked by one of the suspects wielding a kitchen knife, who temporarily broke free after the police had held the men in custody for 30 minutes. Of the four wounded officers, three were stabbed and the other suffered a broken ankle. None of the injuries were life-threatening. In London, Prime Minister Tony Blair said he was shocked and saddened. "It is an appalling tragedy and wicked in the extreme," he said. **The news came after word from the English Channel city of Bournemouth that six people arrested Monday by antiterrorism police and initially thought to be connected to the London ricin case were found instead to have been involved in a terrorism hoax and possible immigration infractions. The police would not elaborate on the incident, but terror charges were withdrawn against all six, and police blamed reports of their possible involvement with ricin to newspaper speculation.** Tonight, Alan Green, the Greater Manchester assistant chief constable, said the stabbing victim died at North Manchester General Hospital after having received emergency treatment at the scene. Green said he was unable to give details about the operation tonight but could confirm that the raid was tied to arrests by Scotland Yard in recent days in London. A spokeswoman for the Manchester police said the three men arrested tonight were North Africans.

Source: <http://www.nytimes.com/2003/01/15/international/europe/15LOND.htm>

33. *January 15, Wall Street Journal* — **Two Silicon Valley cases raise fears of Chinese espionage.** Federal agents are investigating whether Chinese companies were involved in alleged attempts to steal vital commercial technologies from two Silicon Valley companies. **Authorities see the two cases as part of an emerging pattern of trade-secrets theft aimed at helping Chinese enterprises. In both instances, the alleged thieves were arrested at San Francisco airport as they tried to board flights to China. The technologies at issue include computer-chip designs and software used to find oil and gas, executives of the allegedly targeted U.S. companies and federal officials say. Investigators haven't found any links in the cases to China's state security apparatus, but they have uncovered ties to other government-controlled entities. Central- and local-government entities own most businesses in China, but they often are autonomous and pursue profits aggressively.** A Chinese Embassy official in Washington said there was no central-government involvement in the cases, calling them isolated instances carried out by individuals. "There are several cases like this now in Silicon Valley," the official said. Likewise, a consular spokeswoman in San Francisco called such incidents "personal behavior [that has] nothing to do with the China government."

Source: <http://online.wsj.com/article/0..SB1042580870500857584.00.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 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.