



National Infrastructure Protection Center NIPC Daily Open Source Report for 06 January 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports utilities nationwide are asking states for rate hikes to cover the cost of anti-terrorism security measures. (See item [1](#))
- The New York Times reports a former manager of a tax preparation office and three of her friends have been charged with running an identity-theft ring that used the names of company customers to obtain credit cards illegally and steal thousands of dollars in cash and merchandise. (See item [10](#))
- The Associated Press reports the government is proposing a plan that would require detailed information about every person who comes to or leaves the country by plane or boat, and for the first time will require U.S. citizens to fill out forms detailing their comings and goings. (See item [14](#))
- Editor's Note: Beginning today, the NIPC Daily Open Source Report is being published in PDF format. The reader is free and can be downloaded from <http://www.adobe.com/products/acrobat/readstep2.html>.
- Editor's Note: Beginning today, the NIPC Daily Open Source Report is aligned to cover the critical infrastructure sectors as identified in the National Strategy for Homeland Security. Currently covered sectors, which were set forth in Presidential Decision Directive 63, are included in the new format. The new Sector alignment is as follows: Agriculture, Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information and Telecommunications, Energy (to include Electric Power, and Oil and Gas), Transportation, Banking and Finance, Chemical Industry and Postal and Shipping. Readers wishing to comment on the contents or suggest additional topics and sources should contact Melissa Conaty at 202-324-0354 or Kerry J. Butterfield at 202-324-1131. Requests for adding or dropping distribution to the NIPC Daily Open Source Report should be made through the Watch and Warning Unit at nipc.watch@fbi.gov.

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](#)

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 05, Associated Press* — **Utilities nationwide ask for rate hikes to cover terrorism security costs.** The government, fearing that terrorists might try to sabotage power stations or poison water supplies, has urged utilities to beef up security – at a significant cost. **Therefore, a growing number of utility companies are asking states for permission to add security fees to customers' bills to recover the cost of protecting themselves against possible terrorist attack.** A survey conducted last year by the National Regulatory Research Institute and released in November **said at least 13 states had been approached by a utility for a rate adjustment related to security costs.** Last week, the Pennsylvania–American Water Co. told 600,000 customers that it had asked regulators for permission to charge 4 cents a day for terrorism–protection measures. **Most of the money will pay for more security patrols around reservoirs and filtration plants.** "Since Sept. 11 we have remained on heightened security and hope to recoup our costs related to security," company spokeswoman Joi Corrado said. Natural gas supplier PG Energy is considering a similar move, spokeswoman Donna M. Gillis said. **"We are evaluating all our options to recover costs related to increased expenses we incur due to tightened security,"** she said.
Source: http://story.news.yahoo.com/news?tmpl=storyp_woen_po/na_gen_us_terrorism_surcharge_1
2. *January 04, New York Times* — **Regulators' wariness kept a damaged A–plant open.** Three months before workers refueling an Ohio nuclear reactor discovered last year that its lid had rusted nearly all the way through, the staff of the Nuclear Regulatory Commission (NRC) drafted an order to close it for inspection. But the order was never issued, because the staff doubted its authority to close the plant, did not want to impose unnecessary costs on the owner, and was reluctant to give the industry a black eye, according to an internal commission report released today. **The report, by the commission's inspector general, concluded that the staff had been too hesitant and that a policy adopted by the NRC in the mid–1990's to take costs into account when setting regulatory requirements was in conflict with the commission's goal of maintaining reasonable assurance of public safety.** The report, dated Dec. 30, was issued today after an account about it appeared this morning in the Cleveland daily *The Plain Dealer*. Its sharp criticism of the commission's staff concerned the belated nature of the shutdown of the Davis–Besse reactor, near Toledo, last year. Other reactors of the same design had been found to have cracks in parts attached to the lid, and the commission wanted all such plants inspected by Dec. 31, 2001. The operators of the Davis–Besse plant wanted to wait until March 2002, when the reactor was scheduled to be shut anyway for refueling. **When the plant finally closed, on a compromise date in February 2002, engineers and workers were shocked to find that cracks of the kind the commission staff had suspected there had let acidic water leak onto the head, where it had eaten away a**

70–pound chunk of steel six inches thick. Only a layer of stainless steel about a quarter–inch thick had prevented the cooling water from spewing out of the vessel head, in a leak that could have proved catastrophic. The corrosion was the most extensive ever found at an American nuclear plant.

Source: http://www.nytimes.com/2003/01/04/national/04NUKE.html?ex=1042714_144

- 3. *January 03, Washington Post* — Analysts: U.S. risks fuel spike with closed reserve.** The United States is taking a gasoline price gamble by declining to open its emergency oil reserve despite an export crisis from Venezuela that has begun to cut deep into U.S. oil supply, energy analysts said Friday. **U.S. refiners, including Citgo and Amerada Hess, have requested oil from the U.S. Strategic Petroleum Reserve (SPR), citing the loss of 2.7 million barrels per day of crude from strike–bound Venezuela.** But so far the requests have been turned down by a White House preoccupied with Iraq. **Fears abound that, without a release from the SPR, U.S. refiners may be hard pressed to pad gasoline supplies enough to avoid a price spike this summer when drivers return to the roads for the vacation season.** Oil supplies from OPEC–member Venezuela – which normally supplies around 13 percent of U.S. gasoline imports – have been shut off since Dec 2 by an open–ended national protest against leftist president Hugo Chavez. **U.S. stocks of crude oil have fallen close to their lowest level in 26 years.** Major U.S. refineries, which normally depend on Venezuelan crude, have had to lower production of fuels because of rising crude feedstock prices. "The worries that some have is that you've taken out a significant chunk of exports from Venezuela into the U.S. as well as the regional market, which needs to be supplied from somewhere else," said Jan Stuart of ABN Amro. **"The run–up to driving season looks tighter than it did last year and brings back memories of 2000 and 2001,"** when gasoline prices spiked due to low supplies, Stuart added.

Source: <http://www.washingtonpost.com/wp–dyn/articles/A5539–2003Jan3.html>

- 4. *January 03, Platts Energy News* — U.S. warns of big run cuts if Venezuela strike continues.** **U.S. refineries are potentially a week away from major run cuts because of a lack of crude imports from Venezuela,** the U.S. Energy Information Administration said in a report released Thursday. For the week ended Dec 27, when Venezuelan exports were virtually nonexistent, U.S. crude imports averaged 7.6–mil b/d, the lowest average since the week ended Jan 28, 2000, the EIA noted. With refining margins still "relatively good right now," refiners drew upon inventories to partially make up for the reduction in imports. **As a result, U.S. crude inventories dropped 9.1–mil bbl from the prior week to stand at 278.3–mil bbl, just 8.3–mil bbl above what EIA considers the "lower operational inventory level."**

Source: <http://www.platts.com/stories/oil1.html>

- 5. *January 03, Atlanta Journal–Constitution* — Scandal hits Japanese nuclear sites.** A scandal so severe that top executives have resigned in shame has plunged Japan's nuclear power industry into crisis, with many power plants shut down and companies having to import fuel for the winter ---- all because of cover–ups and lies concerning cracks and leaks at the plants. The magnitude of the scandal is declared in an apology issued Dec. 11 by the Tokyo Electric Power Co. (TEPCO) when it expressed regret not only to people who live near its nuclear plants but also "to all members of society." In Japan, debate continues about whether the cracks ---- many discovered and repaired without government regulators' knowledge ---- presented a danger. TEPCO, and to a lesser extent several other utilities, discovered cracks in components of their

plants — particularly shrouds, the stainless steel structures that separate the flow of cooling water inside the reactor. **Attributing many of the problems to stress–corrosion cracking, which increasingly requires replacing parts at nuclear plants worldwide, TEPCO hid the evidence, keeping its inspection reports from government regulators. The most extreme case involved not just concealment of cracking — which the power plants maintain was unrelated to safety — but the rigging of two consecutive annual tests for leaks at TEPCO's Fukushima Nuclear Power Station.** TEPCO employees secretly pumped air into the reactor to minimize the leak rate. **Had the Japanese government known, it most likely would have shut down the reactor.**

Source: http://www.accessatlanta.com/ajc/epaper/editions/today/news_e35172f4a3dcf09d00c8.html

- 6. *January 03, Reuters* — Australia considers one–km tall power tower.** The world's tallest man–made structure could soon be towering over the Australian outback as part of a plan to capitalize on the global push for greater use of renewable energy. **By 2006, Australian power company EnviroMission Ltd hopes to build a 1,000 m solar tower in southwest New South Wales state.** The 200–megawatt solar tower, which will cost 1 billion to build, will be of a similar width to a football field and will stand in the center of a massive glass roof spanning seven kilometers in diameter. **Despite its size, the technology is simple — the sun heats air under the glass roof, which slopes upward from three meters at its outer perimeter to 25 meters at the tower base. As the hot air rises, a powerful updraft is also created by the tower that allows air to be continually sucked through 32 turbines, which spin to generate power 24 hours a day.** EnviroMission hopes to begin construction on the solar tower before the end of the year and be generating enough electricity to supply 200,000 homes around the beginning of 2006. The company also hopes the project will save more than 700,000 tons of greenhouse gases a year that might otherwise have been emitted through coal or oil–fired power stations. The tower has received the support of the Australian and New South Wales governments, which have defined it as a project of national significance. EnviroMission plans to build the tower in remote Buronga district in New South Wales. **It will generate about 650 gigawatt hours (GWh) a year towards Australia's mandated renewable energy target, which requires electricity retailers to supply 9,500 GWh of renewable energy a year by 2010.**

Source: <http://in.news.yahoo.com/030103/137/1zoxs.html>

- 7. *January 01, BBC* — Bulgaria to store radioactive elements for 35 years after reactors closed. On 31 December the first and second reactors of the Kozloduy nuclear power plant were disconnected from the country's power grid in accordance with the decision of the Council of Ministers.** Yuliyana Stoyanova reports that the first two 440–megawatt reactors of the Kozloduy nuclear power plant were stopped within 24 hours. According to the instruction of the Central Control Administration the second reactor was the first to be disconnected from the country's power grid. **The necessary technological procedures which will allow the safe storage of the reactors for a long period of time are underway.** The strategy adopted by the Central Control Administration includes the postponed dismantling of the first and second reactors, **and the safe storage of the reactors' radioactive elements for a period of about 35 years. Afterwards the reactors will be dismantled and destroyed.** According to Energy Minister Milko Kovachev, who was at the Central Control Administration during the stoppage of the second reactor, **the closure of the first two reactors of the**

Kozloduy nuclear power plant will not prompt an electricity shortage nor an electricity price increase. Text of report by Bulgarian radio on 1 January:

Source: http://www.energycentral.com/sections/newsroom/nr_article.cfm?id=3546366

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

- 8. *January 02, National Journal's Technology Daily* — Homeland Security contractors may get indemnification.** The defense and technology industries are hopeful that in the coming weeks, the Bush administration will commit to picking up the tab for some future lawsuits involving homeland security products and services provided to government. The White House is expected to circulate a draft modifying a longstanding executive order under which the Defense secretary and agency heads may choose to indemnify contractors for unusually hazardous products. The modifications to Public Law 85–804 would extend the indemnification to homeland security providers. "We look forward to working with the administration in their consideration of the executive order. **These actions together will ensure the ability of the defense and technology sectors to actively participate in homeland security,**" said David Colton, vice president at the Information Technology Association of America, which represents technology and defense contractors. Industry sources said indemnification would give additional confidence to company management to support their company's participation in homeland security procurement opportunities.

Source: <http://www.govexec.com/dailyfed/0103/010203td2.htm>

- 9. *December 31, Government Computer News* — Agencies could be penalized for late payments to contractors.** Agencies that make late interim payments to contractors on cost reimbursement contracts now are required to pay an interest penalty, according to an Office of Management and Budget final rule published in the Federal Register on **December 30**. The regulation implements Section 1010 of the National Defense Authorization Act of 2001. OMB has worked on the rule for two years after publishing two interim final rules in December 2000 and October 2001. **Vendors are now eligible for interest payments if agencies do not reconcile invoices in 30 days, the new rule says.** All contractors with cost reimbursement contracts for services that include interim payments due after Dec. 15, 2000, are eligible for interest payments. An interim payment is defined as allowable costs incurred in the performance of the contract. OMB still must publish a regulation on how to compute interest.

Source: http://www.gcn.com/vol1_no1/procurement/20750-1.html

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

Banking and Finance Sector

10. *January 03, The New York Times* — **Former tax preparation manager accused in identity–theft ring. A former manager of a tax preparation office in White Plains, NJ and three of her friends have been charged with running an identity–theft ring that used the names of company customers to obtain credit cards illegally and steal thousands of dollars in cash and merchandise, the authorities said yesterday.** At least 27 customers were victims of the scheme between July 2001 and the spring of 2002, according to a complaint by the United States attorney for the Southern District of New York, James B. Comey. A spokesman for the office, Marvin Smilon, said the investigation was continuing and the exact amount stolen had not been determined. The arrests were first reported yesterday in The Journal News. Mr. Kezer said the four suspects used customers' personal information to obtain credit cards and then make purchases and withdrawals from A.T.M.'s with them. **The four suspects were charged on Dec. 18 with conspiracy to commit both mail fraud and credit card fraud, and each was released on a \$25,000 bond Dec. 19, Mr. Smilon said.**

Source: <http://www.nytimes.com/2003/01/03/nyregion/03THEF.html>

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

Transportation Sector

11. *January 03, Detroit Free Press* — **Express travel lanes prepared for border. The Detroit–Windsor Tunnel will begin accepting applications Monday for commuters who want to use an electronic express lane. The program, also planned for the Ambassador Bridge, allows preapproved U.S. or Canadian citizens to bypass manned inspection booths with a photo identification card.** The program, called NEXPRESS Added Value could cut travel time through the tunnel in half, said Neal Belitsky, vice president of tunnel operations. To take part, commuters must apply for a government–issued personal photo identification card that eliminates routine questioning at Canadian and U.S. customs booths. **Applicants for NEXUS cards must meet detailed requirements, including security checks, and pay \$50 for a 5–year membership.**

Source: http://www.freep.com/news/mich/date3_20030103.htm

12. *January 03, Federal Computer Week* — **NYC transit help in the wings.** New York City averted a public transit strike recently, saving commuters and residents a metropolitan–size headache of getting around. But if it had come to that, the city was ready to help idle people find their way. A week before the scheduled strike, the city's Office of Emergency Management, the Department of Information Technology and Telecommunications, and Frankfort, Ky.–based PlanGraphics Inc. designed and developed an interactive online map that enabled users to view various alternative transportation options and vehicular restrictions. Although the application was subsequently deactivated, **it's available should a similar situation occur in the future. The system can highlight bicycle and pedestrian access sites, carpool staging areas, rail lines and stations, ferry stops and routes, including contingencies, as well as carpool–only routes and other road restrictions. The application is based on the city's Emergency Management Online Locator System, which allows New Yorkers to find hurricane evacuation routes or cooling centers during a heat wave.**

Source: <http://www.fcw.com/geb/articles/2002/1230/web-nyc-01-03-03.asp>

13.

January 03, Reuters — **Paris airport worker used by militants.** A Paris airport baggage handler being probed after weapons were found in his car may have been used by militants to transport top class explosives and guns, Le Parisien newspaper said on Friday. Quoting investigators, Le Parisien said **weapons found in the car of Abderazak Besseghir, a Frenchman of Algerian origin, were highly sophisticated and probably came from abroad.** "It is very high quality material... it is difficult to find," an unnamed investigator told Le Parisien. **"It is hard to see how he could have got that alone."** Le Parisien quoted investigators as saying he may have been used by a larger network to transport the arms after they arrived at the airport where he worked. Le Parisien article is available at <http://www.leparisien.fr/home/info/permanent/article.htm?themeid=515676>
Source: <http://www.alertnet.org/thenews/newsdesk/L03237277>

14. *January 03, Associated Press* — **U.S. proposes visitor tracking rules. The government wants detailed information about every person who comes to or leaves the country by plane or boat, and for the first time will require U.S. citizens to fill out forms detailing their comings and goings.** Under rules proposed Friday, the information would be sent electronically to the government for matching against security databases. The public will have a month to comment on the plan and the final regulations will take effect later this year. The proposal requires all passengers arriving or departing, as well as crew members, to provide this information: name, date of birth, citizenship, sex, passport number and country of issuance, country of residence, U.S. visa number and other details of its issuance, address while in the United States, and, where it applies, alien registration number. **All airlines, cargo flights, cruise ships and other vessels carrying crew or passengers will be affected, with the exception of most ferry boats.**

Source: http://www.accessatlanta.com/ajc/news/ap/ap_story.html/National/AP.V9788.AP-Tracking-Travel.html

[[Return to top](#)]

Postal and Shipping Sector

15. *January 03, Reuters* — **Canadian anthrax scare proves false. Powder contained in letters addressed to Canada's controversial firearms registry tested negative for anthrax early on Friday after a scare that sent two postal workers to hospital for examinations, police said.** The employees discovered what police and fire officials initially determined as possible anthrax late on Thursday at a sorting outlet in west Edmonton, Alberta. But subsequent testing proved the substance in two letters did not contain the potentially lethal spores, Edmonton Police Sgt. Dan Doerksen said. "We're checking other packages, but we're treating everything now as a hoax," he said.

Source: <http://www.nytimes.com/reuters/international/international-crime-canada-anthrax.html>

[[Return to top](#)]

Agriculture Sector

16. *January 03, Associated Press* — **Canada, Mexico ban California poultry.** Canada and Mexico have banned shipments of poultry and poultry products from California because of the outbreak of exotic Newcastle Disease, the California Farm Bureau said. **State farm officials said Canada will stop all shipments of poultry and its products from California for 14 days. Mexico, the state's leading export market for poultry, also called for a similar ban.** The California Poultry Federation, which represents about 160 poultry farmers, was lobbying for the bans to be modified to include only six quarantined counties in Southern California. Source: http://abcnews.go.com/wire/US/ap20030103_349.html

17. *January 02, San Bernardino Sun* — **Duck ranchers take precautions. Operators of the largest duck ranch in San Bernardino, California have heightened security because of a bird disease that is causing the eradication of more than one million chickens.** Company officials with Woodland Farms say they have increased security to protect the roughly 350,000 ducks they own on four ranches in the Inland Empire. Woodland Farms employees are monitoring the ranches to ensure that all sanitization and bio–security measures are followed, said Dick Jones, company president. **While much of the focus on exotic Newcastle disease has been on its effect on the chicken industry, most birds can carry the highly contagious disease, including ducks and ostriches.** Ducks are the second largest poultry industry in San Bernardino County, followed by ostriches, according to January 2002 statistics from the county Department of Agriculture and Weights and Measures. **According to the statistics, there were more than 4.1 million chickens, 412,000 ducks and 300 ostriches in the county in 2002.** Source: <http://www.sbsun.com/Stories/0.1413.208%257E12588%257E1086799.00.html>

[[Return to top](#)]

Food Sector

18. *January 02, Reuters* — **Salmonella egg bacteria on the rise in U.S. Southeast.** Outbreaks of a potentially fatal form of salmonella linked to consumption of raw and undercooked eggs are on the rise in the U.S. Southeast, an increase that has puzzled federal health officials, who called on Thursday for expanded efforts to prevent the spread of the bacteria. **In a study published in its weekly morbidity and mortality report, the Centers for Disease Control and Prevention (CDC) said salmonella enteritidis infections had jumped 50 percent in southeastern states in 2001 compared to the previous year.** The CDC said it was not clear why the salmonella bug was becoming more common in a region extending from Delaware to Florida. It noted that other parts of the nation had reported stable or declining infection rates. **The number of U.S. infections overall has fallen by about 50 percent since peaking in 1995 at 3.8 per 100,000 people.** "I don't think it's necessarily something that the Southeast is not doing that the other places are doing," said Dr. Padmini Srikantiah of the CDC's National Center for Infectious Diseases. "The nature of these sorts of epidemics is that we may see increases in certain areas and decreases in others at different times," said Srikantiah, who nevertheless noted that efforts to monitor and prevent the bacteria needed to be strengthened. The CDC report can be found at <http://www.cdc.gov/od/oc/media/mmwrnews/n030103.htm#mmwr1>. Source: <http://www.reuters.com/newsArticle.jhtml?type=topNews4802>

[[Return to top](#)]

Water Sector

Nothing to report.

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

Public Health Sector

19. *January 03, Associated Press* — **Federal scientists study West Nile virus. Scientists at the U.S. Centers for Disease Control and Prevention have had to sharply shift the focus of their work toward West Nile virus that is spreading across the country.** Lab officials say their workload increased dramatically since West Nile virus first appeared in 1999. "Our workload has been a lot, and there is no sign that it is going to let up," said John T. Roehrig, chief of the arbovirus diseases branch of the CDC's Division of Vector-Borne Infectious Diseases. **West Nile previously received the same attention as countless diseases affecting the global community. Now, at the CDC's primary West Nile virus research facility, up to 90 percent of the lab's time and resources are devoted to this disease.** The emphasis on West Nile comes while the lab also tries to address its responsibility for research on plague and tularemia, both highly infectious agents with potential for use in bioterrorism. **Lab scientists are trying to develop better diagnostic testing for West Nile virus. Other research projects include new vaccines for horses and possibly birds, and studies of how the virus may be transmitted between humans through breast milk, blood transfusions, and organ donations.**

Source: <http://www.billingsgazette.com/index.php?id=12003/01/03/build/health/cdclab.inc>

20. *January 03, Clarion-Ledger* — **Hypothesis on West Nile virus confirmed. On Thursday, scientists at the Methodist Rehabilitation Center (MRC), in Mississippi, said their hypothesis that the virus targets the gray matter of the spinal cord has been confirmed through pathological research.** MRC researchers said the data, discovered after conducting tests on tissue samples taken from the bodies of West Nile virus victims, bolsters what they clinically observed in patients treated at Methodist Rehab. **Earlier this year, MRC scientists were the first to report that the West Nile virus was causing polio-like paralysis in some of its victims.** Prior to the findings, national guidelines emphasized that West Nile virus was an attack on the brain and could cause encephalitis and meningitis. **The recovery center's research shows the virus can also attack the motor neurons of the spinal cord that control muscle functions, causing severe muscle weakness.** Researchers said their goal is to gather as much information as possible about how the virus targets humans so better long-term treatment methods can be developed.

Source: <http://www.clarionledger.com/news/0301/03/m03.html>

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

Government Sector

21. *January 03, Government Computer News* — **CIO Council reminds agencies to protect architecture data. The CIO Council Thursday reminded government agency CIOs to**

guard their enterprise architecture information and applications as closely as their core systems. Energy Department CIO Karen Evans, vice chairwoman of the council, said the memo to CIOs was a pre-emptive step. She said some agencies have been concerned about the integrity of their architectural plans after federal agents raided Ptech Inc. of Quincy, Mass., last month. Ptech provides enterprise architecture modeling software to various government agencies. **Although the vendor was cleared of wrongdoing and there were no problems with its software, the situation made "everyone stop and think about how they were securing their EA information," Evans said.** The council noted that **architecture information should be considered mission-critical, and that agencies should use measures outlined in the Government Information Security Reform Act,** which will evolve into the Federal Information Security Management Act. The full text of the memo is available at http://www.cio.gov/documents/Enterprise_Architecture_Software_memo.doc
Source: http://www.gcn.com/vol1_no1/daily-updates/20764-1.html

[[Return to top](#)]

Emergency Services Sector

22. *January 03, Washington Post* — **Fake-ID arrest led to FBI hunt. An accused immigrant smuggler who is jailed in Canada has told authorities that he was offered large sums of cash to help five foreign nationals illegally enter the United States from Pakistan,** a revelation that set off this week's manhunt for five men the FBI fears may be planning terrorist attacks, U.S. officials said. Michael John Hamdani, who was arrested three months ago in suburban Toronto, allegedly with \$600,000 in fake traveler's checks and a sophisticated passport counterfeiting lab, is the original source of the information that five men and perhaps others had arranged to travel from Pakistan to England, then to Canada and, finally, the United States, U.S. officials said Thursday. **U.S. authorities say that they still do not know where the five men are, and are concerned that the men may be planning a terrorist strike in this country. U.S. officials acknowledge being frustrated by what they do not know about the case.** Hamdani, who U.S. officials say has had past dealings with suspected terrorists, has told investigators he was contacted months ago by people offering at least \$20,000 to \$30,000 for each man he was able to transport from Pakistan into the United States, officials said.
Source: <http://www.washingtonpost.com/wp-dyn/articles/A3629-2003Jan2.html>

[[Return to top](#)]

Information and Telecommunications Sector

23. *January 03, Government Computer News* — **Hacker of federal Websites could spend a decade in jail.** NASA's inspector general has announced that **William Douglas Word of Pelham, Alabama faces up to ten years in prison after pleading guilty to defacing sites of NASA, Defense Department agencies, Interior Department and the International Trade Commission, among others,** according to a grand jury indictment handed down in the U.S. District Court for the Northern District of Alabama. Much of the criminal activity occurred in late 1999, the inspector general said. The NASA Office of Inspector General (OIG) investigated the crime together with the Defense Criminal Investigative Service, the Naval Criminal

Investigative Service and the FBI. James E. Phillips, U.S. attorney for the Northern District of Alabama, prosecuted the case. Word "was rolled up in a group of hackers that decided to turn themselves in after we got close to confronting them," a NASA official said. **"This was the typical hacker case where they were demonstrating their skills."** Word is to be sentenced April 24.

Source: http://www.gcn.com/vol1_no1/daily-updates/20766-1.html

24. *January 03, CNN* — **Mystery man named in Xbox hack contest. A longtime Microsoft opponent has emerged as the mystery backer and mastermind behind a contest that offers \$200,000 to anyone who successfully hacks into the software giant's Xbox video game console, a top technology news site reported.** Michael Robertson, a former dot-com entrepreneur and now chief executive of U.S. software company Lindows.com, revealed himself as the anonymous donor and contest's creator in an interview on Thursday with CNET News.com. **Last July, Robertson anonymously dangled the prize money to any programmers who could successfully hack into the Xbox and adapt it so that it would run on the Linux operating system, an emerging competitor to Microsoft's Windows operating system.** Robertson recently extended the deadline as no group has fully mastered the challenge. The hack contest goes beyond a sporty challenge. **Linux proponents have long charged that its freely distributed operating system, designed and modified by mainly unaffiliated groups of programming enthusiasts, is an important step for the future development of computing devices.** They argue that the market dominance of Windows, which is the operating system on more than 90 percent of all PCs, gives Microsoft and a small number of its business partners unfair and anti-competitive control in the design of the growing number of devices that come equipped with computing capabilities. Robertson's firm Lindows.com is a start-up that **aims to promote the use of the Linux open-source operating language in computer systems, a move that would challenge Microsoft's dominant Windows operating system.**

Source: <http://www.cnn.com/2003/TECH/fun.games/01/03/bounty.game.reut/index.html>

25. *January 02, National Journal's Technology Daily* — **IT systems key to success of Department of Homeland Security. Strong information technology systems will be crucial to the success of the new Department of Homeland Security, according to the General Accounting Office (GAO).** The GAO report (03-260), released December 24, found that **federal agencies have made progress in addressing their homeland security missions** since the September 11, 2001, terrorist attacks, and that information sharing between federal agencies has increased. But GAO said **federal agencies still face many challenges, such as improving their collaboration with state and local officials and with the private sector.** Twenty-two existing federal agencies and offices will move into the new DHS, which also will include an Office of State and Local Coordination and a liaison official for the private sector. **GAO estimated that the full transition to the new department could take five to 10 years,** and recommended that the Office of Management and Budget (OMB) work with the department to implement the appropriate management systems. **"Strong financial and information technology systems will also be critical to the success of [the DHS] and other organizations with homeland security missions."**

Source: <http://www.govexec.com/dailyfed/0103/010203td3.htm>

26. *January 02, ZDNet* — **Virus hoaxes continue to fool computer users.** Fuelled by concern over genuine threats such as Klez, Bugbear and Magistr, **computer users are continuing to**

fall for false warnings of non-existent viruses. These hoaxes typically warn the reader not to open an e-mail with a certain subject line, or to immediately delete a particular file on their hard drive, because they contain a virus. They will also tell the reader to forward the warning to their friends and colleagues. Even though these hoaxes didn't encourage the reader to delete files from their machine, they are harmful because they waste both time and bandwidth. All the major anti-virus companies include information on such hoaxes on their Web sites.

Source: <http://zdnet.com.com/2100-1105-979042.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), 1433 (ms-sql-s), 80 (http), 139 (netbios-ssn), 27374 (asp), 135 (???), 53 (domain), 4662 (???), 445 (microsoft-ds), 21 (ftp) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

27. *January 03, New York Times* — Recent attacks in Yemen seen as sign of large terror cell.

The investigation into two high-profile attacks in Yemen in the last week, including the killing of three American missionaries, **suggests that a larger cell of Islamic militants has been planning to strike at other foreigners as well as secular-minded politicians, a security official said Friday.** The official said there is little evidence of direct involvement by Al Qaeda, but a government-owned weekly newspaper reported today that Abed Abdel Razzak Kamel, the man arrested in connection with the killing of the Americans on Monday, has admitted meeting with Qaeda operatives in 1997. **Investigators are saying that the killings were connected and that the two suspects appear to be part of a group of Islamic militants, headed by Mr. Jarallah.** The security official said today that messages on audiotape made by Mr. Jarallah were confiscated this week. On the tapes, **Mr. Jarallah instructs members of the group to carry out other attacks. Among the targets, the official said, were journalists promoting secularism, Westerners in Yemen and the heads of several political parties.**

Source: <http://www.nytimes.com/2003/01/03/international/middleeast/03YEME.html>

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.