



National Infrastructure Protection Center NIPC Daily Open Source Report for 04 February 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- Aviation Week and Space Technology reports the Transportation Security Administration's new rules require foreign pilots seeking to undergo training in the U.S to submit a request for authorization prior to attending classes and following flight training courses in the U.S. (See item [9](#))
- The New York Times reports the Red Cross has announced the recent quarantine on donated blood has been expanded, since an unidentified white fatty substance has been found in three samples of donated blood in Tennessee. (See item [17](#))
- The Washington Times reports the Bush administration is establishing a national biometrics identification system to prevent terrorists from gaining legal entry into the country, and suggests international standards should be established. (See item [19](#))
- eWeek reports Symantec has published a report indicating that as the number of software vulnerabilities increases, most attackers search for a few vulnerabilities to exploit and will abandon their efforts if these vulnerabilities are unavailable. (See item [21](#))
- Note from the Editor: As of 3 February, the NIPC Daily Open Source Report is being distributed through a new list service. While significant effort has been done to ensure smooth transition, problems are bound to occur. Please notify nipcdailyadmin@mail.nipc.osis.gov with any comments, concerns, questions, or problems.
- Note from the Editor: The ISS AlertCON was changed from level 2 to level 1 yesterday. See the Internet Dashboard for more details.
- Note from the Editor: Both the PDF and Word versions of the daily are posted to the NIPC Web Site at <http://www.nipc.gov/dailyreports/dailyindex.htm>

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. *February 03, U.S. Department of Transportation, Office of Public Affairs* — **Department of Transportation awards \$627,000 for pipeline safety research. Ellen G. Engleman, Administrator of the U.S. Department of Transportation's Research and Special Programs Administration (RSPA), today announced three research contracts as part of a government–industry partnership to improve pipeline safety and reliability through technology.** The awards implement the second phase of a new competitive pipeline safety research partnership. DOT's awards address pipeline enhanced operations, controls and monitoring solutions, and provide \$627,000, which is matched through the partnership to make approximately \$1.3 million available for research. "Public confidence is a major measure of success for this aggressive program of technology development," said Administrator Engleman. "Technology is a key element in improving the safety and reliability of the growing pipeline infrastructure that is critical to our economy and way of life." **A government–industry leadership team that includes the U.S. Departments of Energy and Interior, and several state agencies, helped DOT build the blueprint for the new program and move from concept to award in one year. The awards are for technologies that are ready for commercialization in three to five years, to move quickly to enhance pipeline safety.**
Source: <http://www.dot.gov/affairs/rspa0303.htm>
2. *February 03, Wall Street Journal* — **Cleanup of nuclear sites to face first big test. Building 771, a bunker–like structure in Rocky Flats, CO, once known as "the most dangerous building in America," soon will be pulverized, its lethal debris sealed in barrels and hauled away.** The defense complex at Rocky Flats was the machine shop of the Cold War, and Building 771 was where hydrogen–bomb triggers were made. Now the site presents the first big test of the nation's most complex, costly and dangerous cleanup project. The Department of Energy is trying to remove toxic and radioactive contamination left at 114 sites around the country that were used for nuclear–weapons production. This sprawling complex of 700 buildings just 15 miles northwest of Denver housed the equipment and foundry used to fashion parts for hydrogen warheads from plutonium and highly enriched uranium. The original plan estimated it would take more than 60 years and at least \$22 billion to dismantle Rocky Flats. **The new plan is to level it by 2006, at a cost of just \$7 billion -- and to try to turn it into a federal wildlife refuge. At Building 771, Kaiser–Hill's site manager, Tom Dieter, figures that by December the structure -- which has the floor space of five football fields -- will be only a memory. By then the dangerous materials will be hauled to dumps in New Mexico and Nevada. The rest of the rubble will be buried under three feet of clean topsoil on site.** Between now and then, his work crews -- many of them dressed in moon suits and working in plastic tents -- will flush out its remaining hazards, which include substantial amounts of nitric acid, asbestos and beryllium. The tight secrecy surrounding the construction of Rocky Flats resulted in few blueprints to describe the innards of the building, so Dieter must depend on long–time experienced workers to pinpoint hazards.
Source: <http://online.wsj.com/article/0..SB1044233441297201664.00.ht>

3. *February 03, South Bend Times* — **There has been no timetable set for the return to service of a Cook Nuclear Plant reactor turned off Wednesday night due to a fire at the main transformer of Unit 1. . The fire that took 35 minutes to extinguish resulted in an automatic shutdown of the reactor and brief activation of the site emergency plan at the American Electric Power plant.** "That will remain off while we continue to investigate repair or replacement of the transformer," AEP spokesman Bill Schalk said Thursday. A security officer with SBI Security was taken to Lakeland Hospital, St. Joseph, due to smoke inhalation, but was treated and released Wednesday night. Oil from the transformer and water from the firefighting efforts combined to overwhelm the oil–containment catch basins and some non–PCB (polychlorinated biphenyls) oil was released to the storm–water system, according to the release. Had such an oil been used in the Cook Unit 1 transformer, it would have led to more significant cleanup requirements, Schalk said, besides that which is already going on. Notification was given to all national, state and local agencies regarding the spill, he said. Last June,, a fire at the plant's switchyard, which routes the generated electricity to AEP's power grid, left a contracted worker with minor injuries.
Source: http://www.energycentral.com/sections/newsroom/nr_article.cf m?id=3619261
4. *February 02, Reuters* — **OPEC moves to fend off decrease in oil prices . OPEC is preparing to fend off any sharp decreases in oil prices in the second quarter, oil ministers said today. Although world oil prices have moved above \$30 a barrel as a result of war fever and political turmoil in Venezuela, an OPEC member, the ministers were warned that markets could tip into oversupply in the second quarter and cause prices to fall. "If there is danger of a glut, we have to meet and rectify the situation," Obeid bin Saif al–Nasiri, the petroleum minister of the United Arab Emirates, said. He said that the Organization of the Petroleum Exporting Countries was concerned about the second quarter. "Typically there is less demand then," he said, "and I hope this increase or the change of the ceiling won't affect it so badly." Nasiri was referring to a decision by OPEC to increase supplies by 1.5 million barrels a day, to 24.5 million, as of Feb. 1, to cover an export shortfall caused by a general strike in Venezuela. Saudi Arabia, the largest producer, said markets were not starved of crude now and vowed that the group would keep pumping enough oil to meet its higher limit.** The Saudi oil minister, Ali al–Naimi, said that Saudi Arabia would make sure that 24.5 million barrels a day was delivered.
Source: <http://www.nytimes.com/2003/02/03/business/worldbusiness/03O IL.html>
5. *February 02, The Record, Hackensack, N.J.* — **New Jersey utilities hope to lock in good rates with Internet auction. The Basic Generation Service (BGS) auction, which begins next Monday (Feb. 10) in cyberspace, was created to lock in future rates for the billions of dollars of electricity that New Jersey's utilities will need, guaranteeing supplies and protecting customers from the volatility of the energy markets. As with eBay selling, bidding is conducted over the Internet, and as with those at Sotheby's, the bids will be in the millions of dollars. But unlike better–known auctions, this one starts high and goes down, down, down, ending only when the lowest bid comes in. The process, administered by a consulting firm hired by the state's electric utilities and monitored by the Board of Public Utilities, could take more than a week, and by the time the bidding is completed, the utilities will have spent billions of dollars and locked in as much as 18,000 megawatts of**

electricity to keep lights and appliances running through 2006. Most consumers are unfamiliar with the concept of BGS, but it has a direct bearing on their lives. As part of New Jersey's deregulation of its energy industry, which opened markets to third-party suppliers 3 years ago, the Legislature required the established utilities to continue providing power to customers who don't switch suppliers or for those left stranded when the alternative supplier pulls up stakes. As it turns out, that includes almost everyone, because competition, after a brief surge when deregulation began in 1999, has virtually disappeared. Few customers ever switched, and most who did, went back to their utilities as most of the competitors who came into the market three years ago have since left the state. **As a result, the four utilities -- PSEJersey Central Power & Light, Orange and Rockland Utilities, and Conectiv -- continue to serve nearly everyone in their territories, just as they did on Aug. 1, 1999, when deregulation's four-year phase-in began.** Last year was the first auction -- before that, the utilities bought power on their own -- so no one knew quite what to expect. The concerns proved to be baseless, as the auction lasted 73 rounds over nine days, with more than 20 qualified bidders participating. The BGS auction is actually two separate, concurrent events. One will be for about 1,700 large industrial users whose rates are based on hourly spot market prices, and the other is for smaller commercial and residential customers, whose prices are fixed.

Source: http://pro.energycentral.com/professional/news/power/news_article.cfm?id=3615299

- 6. February 01, Denver Rocky Mountain News* — **Renewable energy group to push wind, solar power.** National wind energy developers have joined with Colorado and Utah nongovernmental organizations to launch a regional renewable energy trade group. **The Interwest Energy Alliance will advocate public policies that promote renewable energy technologies such as using wind and solar energy for power, said founder Craig Cox. "If given proper public policy support, wind and other renewable energy technologies could provide over \$1 billion of economic development benefits in Colorado alone over the next 20 years," Cox said.** Cox argues that rural areas that have been hard hit in the economic downturn stand to benefit most from the development of wind and other renewable energy sources. Cox said the first goal of the Interwest Energy Alliance will be to advance a renewable portfolio standard in the Colorado and Utah legislatures.

Source: http://pro.energycentral.com/professional/news/power/news_article.cfm?id=3616405

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

- 7. February 03, Department of Defense* — **Fiscal 2004 Department of Defense budget release.** President George W. Bush released on Monday details of his fiscal year (FY) 2004 Department of Defense (DOD) budget. The budget requests \$379.9 billion in discretionary budget authority -- \$15.3 billion above FY 2003. **Global War on Terrorism: In his FY 2003 budget,**

President Bush requested \$10.1 billion for the Department's baseline funding including \$8.2 billion for acquisition and other requirements resulting from the Department's experience in the global war on terrorism, \$1.2 billion for increased air patrols in the continental United States, and \$0.7 billion for implementation of the Nuclear Posture Review. Congress appropriated only \$7 billion of the \$10.1 billion requested. Congress did not appropriate the additional \$10 billion the President requested as a contingency for FY 2003 incremental operations costs related to the global war on terrorism. In the FY 2004 budget, the Department continues to acquire capabilities critical to the war on terrorism. FY 2004 initiatives for force protection and combating terrorism include intrusion detection systems, blast mitigation measures, chemical and biological detection equipment, personal protection gear, waterside security enhancements, harbor patrol boats, regional command systems, mass notification systems, and initiatives to restrict access to DOD installations. Highlights of FY 2004 investment funding for key programs supportive of transformation: **Missile Defense. \$7.7 billion for the Missile Defense Agency to continue research, development and testing of an evolutionary missile defense program focusing on fielding an initial capability in 2004 and 2005, and expanding that capability over time through additional measures and technology infusion. The plan is -- over the next 2 years -- to deploy a limited defense against ballistic missiles: In FY 2004: Includes 10 ground-based interceptors. This would provide initial modest capability against North Korean missiles. In FY 2005: Includes 10 additional ground-based interceptors; up to 20 sea-based interceptors; land, sea and space sensors; and command and control upgrades. This would add modest capability against Middle East threats. The FY 2004 budget also includes \$739 million for Patriot Advanced Capability-3 program, including procurement of 108 PAC-3 systems to protect against cruise missile and tactical ballistic missile attack. **Chemical-Biological Defense Program: \$1.1 billion for the total program, with a \$200 million increase to extend near-maximum chemical-biological protection to 200 installations, increase Army biological detection capabilities, and combat new chemical agent threats.** Additional FY04 Budget materials at:**

<http://www.dtic.mil/comptroller/fiscal2004budget/>

Source: http://www.defenselink.mil/news/Feb2003/b02032003_bt044-03.html

8. *February 03, Aviation Week & Space Technology* — **GPS, Milsatcom assets bolstered as war looms.** The U.S. Air Force is beginning to replenish the GPS, Milstar and Defense Satellite Communications System constellations with critical spacecraft as the navigation and military communications systems are readied to provide unprecedented warfighting capabilities to the U.S. forces arrayed against Iraq. **Nearly \$1.7 billion in new GPS, DSCS, Milstar, Delta and Titan military mission hardware will be launched in operations that began last week and extend to about Feb. 10. In addition, various Air Force satellite control centers are also intensifying system configuration commands to older GPS and military satcom satellites already aloft, to ensure their communications, navigation, attitude control and other systems are at peak performance.** This is especially true at the 2nd Space Operations Sqdn. and 50th Space Wing at Schriever AFB, Colorado, that operate the GPS constellation, said USAF Maj. Mike Mason, chief of GPS operations for Air Force Space Command.

Source: <http://www.awsonline.com/cgi-bin/authenticate.pl?destination=docs/issues/20030203/aw38.htm>

[[Return to top](#)]

Banking and Finance Sector

Nothing to report.

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

Transportation Sector

9. *February 03, Aviation Week and Space Technology* — **TSA's restrictions hit European pilots.** Europeans are increasingly worried by the Transportation Security Administration's restrictive policy applied to foreign pilots seeking to undergo training in the U.S. **According to the TSA's new rules, aliens have to submit a request for authorization prior to attending classes and following flight training courses in the U.S. The TSA has up to 45 days to ratify or reject demands.** "The rule is extremely restrictive; it prohibits provision of training unless approved by the attorney general," said Kurt Edwards, the FAA's Paris-based senior representative. The screening process is managed by the Justice Dept. in cooperation with the FAA and flight centers, while a TSA team retains the power to decide who can or cannot get training in the U.S. **The TSA's rule covers pilots seeking training on aircraft up to 12,500-lb. maximum takeoff weight. However, additional regulations covering heavier aircraft, including commercial transports, are expected to be implemented in the next two months, Edwards said.** During a meeting in France last week, the European Business Aviation Association's team expressed serious concerns about rules prohibiting unrestricted access to U.S. training facilities. **"Europe's business aviation largely depends on U.S. flight centers because 70% of the total business aircraft fleet is based in the U.S. It means that [most] flight training centers equipped with a full range of full-flight simulators are in the U.S.,"** EBAA Chief Executive Fernand Francois pointed out. He added that the current difficulties could have an impact on safety.

Source: <http://www.awsonline.com/cgi-bin/authenticate.pl?destination=docs/issues/20030203/aw45.htm>

10. *February 03, Transportation Security Administration* — **Baltimore–Washington International airport to require boarding passes at the security checkpoint starting Tuesday, Feb. 4.** Under Secretary of Transportation for Security Adm. James M. Loy announced on Monday, February 3 that **Baltimore–Washington International Airport (BWI), Columbia, MD, is joining more than 145 other airports in participating in the Transportation Security Administration's "Selectee Checkpoint" program.** The program enhances security and convenience by transferring the screening of selectees from aircraft boarding gates to security checkpoints where screening equipment and personnel and law enforcement officers are concentrated. At Baltimore–Washington International Airport, passengers must now have their boarding passes in hand before they reach the security checkpoint. E–ticket receipts, itineraries and vouchers will no longer provide access through the checkpoints, and boarding passes will no longer be issued at the gates. Boarding passes may be obtained at ticket counters, through airline computer kiosks, or at most skycap curbside stations. In addition to a boarding pass, passengers must show a valid government issued photo ID, such as a driver's license or passport at the checkpoint. **In keeping with TSA's multi-level security system at all airports, TSA screeners will now choose gates, flights and passengers at random for additional screening at the gates.**

Source: <http://www.dot.gov/affairs/tsa1003.htm>

11. *February 03, Aviation Week and Space Technology* — **TSA issues new regulation regarding airmen certificates.** Last week as the Transportation Security Administration (TSA) and the Federal Aviation Administration (FAA) adopted regulations on withholding airman certificates from people found by the TSA to be "security threats." Under procedures that drew immediate, mostly heated criticism from pilots, **the FAA will deny a certificate application from -- or revoke a certificate already issued to -- anyone the TSA identifies as a risk.** The TSA will allow people to appeal its initial findings and give U.S. citizens one more layer of review than aliens. In Federal Register notices published Jan. 24, the TSA set up procedures to assess security threats posed by someone who holds or is applying for an FAA certificate. Such a person will receive an initial notification, which will trigger a period in which the person can seek information on the charge and respond to it. If the initial assessment is confirmed—two senior officials, one of them the head of the TSA, will review cases involving U.S. citizens, while aliens will get a single review—the person will receive a final notification and the case will be closed. **The two agencies' rules took effect immediately,** without the usual publication of proposals and public comment. Each said that this was "necessary to prevent a possible imminent hazard to aircraft, persons and property within the United States," and that "notice and comment are unnecessary, impracticable and contrary to the public interest."

Source: <http://www.awsonline.com/cgi-bin/authenticate.pl?destination=docs/issues/20030203/aw44.htm>

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

Postal and Shipping Sector

12. *February 03, New York Times* — **For now, new rules don't snarl Hong Kong port traffic.** Container shipping traffic slowed on Sunday at the sprawling port of Hong Kong, but **maritime officials reported no serious disruptions as the United States Customs Service began enforcing new antiterrorism rules on cargo bound for American ports.** Shipping executives emphasized that the rules had taken effect in the middle of Chinese New Year celebrations, when few containers are shipped. **They warned that problems could still crop up when business returns to normal next week.** Customs officials had said that the new rules could pose a serious problem for Hong Kong's port, the world's busiest, handling nearly a tenth of all containers worldwide. Unlike most ports these days, the Kwai Chung Port has a laissez-faire business culture in which containers are packed and loaded hours before a ship sails, while **most records are still kept on paper and cannot be easily transmitted electronically to the Customs Service.** The new Customs rules require exporters to provide 14 categories of information electronically to Customs officials. The rules technically took effect two months ago, but the Customs Service set Sunday as the date that it would begin collecting fines for violators shipping containers to the United States from any port. The Customs Service is preparing to impose similar rules next year on air, trucking and rail shipments. **Fines start at \$5,000 for the first container sent to an American port in violation of the rules, and \$10,000 for each additional container, with potential extra penalties up to the value of the cargo. In addition, the Customs Service has banned American ports from unloading containers that do not comply with the rules.**

Source: <http://www.nytimes.com/2003/02/03/international/asia/03HONG.html>

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

Agriculture Sector

13. *February 03, CNews* — **Researchers discover new bacterial disease. Researchers have identified a new bacterial disease in muskies caught in Lake St. Clair, Michigan's most popular fishing lake. The disease is called piscirickettsia and first was identified in 1989 in farmed salmon in Chile.** Its first symptom usually is the appearance of small white lesions on the skin, according to the Paris-based Office international des Epizooties, which monitors animal diseases worldwide. **The disease can damage a fish's kidneys, liver and spleen. Until now, the illness has been little seen in U.S. waters.** But Mohamed Faisal, professor of aquatic and animal medicine at Michigan State University, now reports cases in muskellunge caught in lake St. Clair. "We also have to find out how widespread it is," Faisal said. "It can be harmful to the fish. The lesions are also on their reproductive organs. It depends on their resistance." **"It's an emerging disease," Faisal said. "We have it only in several places, one in California and one here in Michigan. It's always like this with a new disease. I guess it will show up in other states."** Faisal said some deaths of fish in hatcheries in southern California and salmon in Canada have been linked to piscirickettsia. **And in Chile, millions of young salmon raised on farms died from the disease in 1989.** But the bacteria's effects on St. Clair muskies are not yet known.

Source: <http://cnews.canoe.ca/CNEWS/Science/2003/02/03/20007-ap.html>

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

Food Sector

14. *February 01, Reuters* — **Food industry seen embracing irradiation. Stung by record recalls of tainted meat last year, the U.S. food industry is stepping up the use of new technology to irradiate meat as an extra protection against deadly bacteria such as E. coli and listeria.** Just a small part of the 9 billion pounds of ground beef sold in the United States last year was irradiated, but the amount is growing rapidly, despite concerns voiced by some consumer groups about the unknown long-term effects on health. **"I would estimate the total volume currently being irradiated under 5 percent of beef production, but we are anticipating an exponential growth curve,"** said Janet Riley, spokeswoman for the American Meat Institute (AMI). Food companies see irradiation as another barrier of protection against bacteria that can cause food-borne illness, especially to protect children, the elderly and those with weakened immune systems. **"Irradiation eliminates 99.9 percent of the pathogens such as E. coli, salmonella and listeria without changing the taste, texture, appearance or nutritional value of the meat,"** said John Fox, associate professor of agricultural economics at Kansas State University. Irradiation is widely used to sterilize many non-food products, including toothbrushes, home-use adhesive bandage strips, and surgical tools, although at doses much higher than used for food. **Irradiation has been used to kill insects in wheat flour since 1963 and used on common kitchen spices since 1983.**

Source: http://abcnews.go.com/wire/Business/reuters20030201_483.html

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

Water Sector

15. *February 03, Water Tech Online* — **Drinking water protection plans certified in Idaho. The Idaho Department of Environmental Quality (DEQ), in coordination with the Idaho Rural Water Association (IRWA), announced certification of drinking water protection plans for a number of communities and drinking water systems.** Drinking water protection plans are designed to provide communities and drinking water systems with tools to protect drinking water supplies from potential sources of contamination, state officials said in a news release. **To achieve certification, communities and drinking water systems must inventory potential contaminant sources and develop management tools and protection measures. The plans also must include contingency measures, protection strategies for new wells or intakes, public outreach activities, and implementation approaches, officials said.** State certification is effective for three years, after which communities and drinking water systems may apply for recertification based on measurement of their implementation strategies, said officials.

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

16. *January 31, Amarillo Globe-News* — **Water rights insurance to be offered. A Houston title insurance company is hoping to put some assurance to water title rights as the availability of water becomes a stickier issue throughout Texas and other western states.** The title insurance company is offering water rights title insurance along with the traditional title service of checking water rights ownership changes to make certain the rights are not tied up in any ownership disputes. **Water rights title insurance works the same way that title insurance does in the sale of a home or other real estate.** The company has not filed any forms or rates with the Texas Department of Insurance, which regulates title insurance.

Source: http://www.amarillonet.com/stories/013103/new_insuranceto.sh tml

[[Return to top](#)]

Public Health Sector

17. *February 03, New York Times* — **Quarantine expands as white substance is found in more blood. Blood in the Nashville, Tennessee region was quarantined yesterday after a mysterious white fatty substance was found in three samples of donated blood, the Red Cross said. The discovery came two days after 110 units containing the substance were found in Atlanta.** No harmful effects on patients have been reported. The substance has not been identified. It is described as floating in sealed blood bags either invisibly in tiny particles or in pea-size globs. "It doesn't appear to be human in origin," said Dr. Christopher D. Hillyer, an Emory University professor who works with the Red Cross. There have been no reports of patients receiving the tainted blood, and officials said they had no idea what would happen if they did. **The Nashville quarantine affects hospitals in parts of Kentucky and Illinois as well as Tennessee, shelving about 70 percent of the region's Red Cross blood supply, said Ryland Dodge, a spokesman.** Hospitals were being notified last night. On Friday, the Red Cross quarantined thousands of units of blood after the 110 units in Atlanta, out of about 4,000 tested, were found to contain the substance. **The U.S. Food and Drug Administration is**

investigating, along with state authorities, the Red Cross, and the U.S. Centers for Disease Control and Prevention.

Source: <http://www.nytimes.com/2003/02/03/health/03BLOO.html>

[[Return to top](#)]

Government Sector

18. *February 03, Office of Management and Budget* — **Department of Homeland Security: fiscal year 2004 budget highlights.** From 2002 to 2004, resources for the agencies and programs moving into DHS grew by more than 60 percent to \$36.2 billion. During the same period, nearly 61,000 staff were added to protect the homeland. **Highlights for 2004 include: About \$500 million to assess the nation's critical infrastructure (e.g., nuclear power plants, water facilities, telecommunications networks, and transportation systems) and to work to ensure that vulnerabilities are addressed; \$350 million in new funding for vigorous research, development, test, and evaluation capabilities that have not existed for homeland security specific projects, such as nuclear and bioterrorism detection technologies; \$373 million for border security and trade initiatives including technology investments along the border such as radiation detection and x-ray machines for inspecting cargo containers; and \$3.5 billion for the Office of Domestic Preparedness to ensure that first responders are properly trained and equipped,** of which \$500 million is for assistance to firefighters, particularly for terrorist preparedness, and \$500 million is for state and local law enforcement anti-terrorism activities. **Overall, the 2004 Budget provides the Coast Guard with a 36-percent increase (\$1.5 billion) over its 2002 Budget.** To increase safety in our seaports, the budget includes \$65 million to deploy six new Coast Guard Maritime Safety and Security Teams to respond to terrorist threats or incidents in domestic ports and waterways. It also provides an additional \$53 million to buy nine Coast Guard coastal patrol boats to serve as vessel escorts into U.S. ports.

Source: <http://www.whitehouse.gov/omb/budget/fy2004/homeland.html>

19. *February 03, Washington Times* — **Biometrics a tool in war on terror.** The Bush administration is establishing a national biometrics identification system to prevent terrorists from gaining legal entry into the country and says international standards should be established. Biometrics identifies people through their physical characteristics: fingerprints, iris scans, voice signatures or facial scans. It can be used with an identity card or the information can be stored in a database. **Through the USA Patriot Act, Congress directed the administration to develop an integrated entry and exit data system at the borders with particular focus on the development of biometric technology. Homeland Security Secretary Tom Ridge negotiated a border deal with Canada in December 2001 to increase security with plans to use biometrics in travel documents.** Testifying before his Senate confirmation hearing recently, Ridge said "ultimately there needs to be an international standard." "I can envision a day in the not-too-distant future where if we are requiring biometric identification for people to come across our borders, then our friends and allies and others may require the same kinds of information as we visit their countries as well," Ridge said. **Ridge could not give a cost estimate to the Senate Governmental Affairs Committee, but said biometrics will be "a significant part of our entry-exit system."**

Source: <http://www.washingtontimes.com/national/20030203-67404832.htm>

20. *February 03, Aviation Week & Space Technology* — **Homeland security demands strain NIMA's resources.** Unfunded homeland security demands are taxing the National Imagery and Mapping Agency, which, along with its intelligence agency counterparts, is in the middle of a difficult balancing act to deal with the military's operational requirements, domestic concerns and the need to modernize. **With the creation of the Homeland Security Dept. late last month, the intelligence agencies now have two large masters to serve, the new bureaucracy and their historic customer, the Defense Dept., notes NIMA director USAF Lt. Gen. (ret.) James R. Clapper. How that will affect the operations of the intelligence agencies isn't clear, he added, noting that there are policy and financial resource issues that have yet to be addressed.** To help with domestic preparedness, NIMA has begun supporting federal and local agencies with geospatial products, which are essentially maps with lots of detailed information. Additionally, specific database requirements for homeland protection are beginning to evolve, Jack Hild, deputy direct for NIMA's Office of the Americas, told a NIMA and Armed Forces Communications and Electronics Assn. meeting. **NIMA has diverted people and money from other projects to jump-start its homeland security efforts, but so far there has been no infusion of funding to address the new needs, Hild noted. The agency has asked for additional money, but those funds go beyond NIMA's allotted budget and would probably require help from Congress. Most of that money would go toward obtaining data, such as imagery.**

Source: <http://www.awsonline.com/cgi-bin/authenticate.pl?destination=docs/issues/20030203/aw37.htm>

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

Emergency Services Sector

Nothing to report.

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

Information and Telecommunications Sector

21. *February 03, eWeek* — **Cyber attacks decline; vulnerabilities surge.** **The number of attacks on Internet-connected machines decreased over the past six months while the number of software vulnerabilities continued to skyrocket,** according to a new report. This supports the conventional wisdom that most attackers search for a few vulnerabilities to exploit and will abandon their efforts if these vulnerabilities are unavailable," the report concludes. The report, published by Symantec Corp., of Cupertino, Calif., is based on data from more than 400 companies. The company said it recorded **more than 2,500 newly identified vulnerabilities in various software products during all of 2002, an 81.5 percent increase over the previous year.** Several factors may have contributed to this increase, including the huge jump in recent years in the number of researchers looking for vulnerabilities. Once again, **attackers in the United States were by far the most eager to exploit those vulnerabilities** and accounted for more than 35 percent of all of the attacks during the reporting period. South Korea, China, Germany and France rounded out the top five. However, the **South Koreans appear to have the most attackers per capita among countries with the largest online populations,** launching 23.7 attacks per 10,000 Internet users. The U.S. is not in the top 10 on this list.

Source: <http://www.eweek.com/article2/0.3959.857011.00.asp>

22. *January 31, New York Times* — **Pentagon and companies in agreement on spectrum.**

Technology companies and the Pentagon have reached an agreement to unlock a swath of spectrum for the next generation of wireless devices, officials said today. Spectrum is measured by its frequency, usually in units of kilohertz, megahertz or gigahertz. The new agreement will give technology companies access to 255 megahertz of unlicensed spectrum around the 5-gigahertz band. The 5-gigahertz range opens a new arena for the industry's next generation of wireless technology, including 802.11a, one of the so-called Wi-Fi standards that is many times faster than the popular 802.11b used in coffee shops, offices and parks across the country for Internet connections. Military and industry engineers worked around the clock for the last several weeks to determine specifications that could both adequately protect the military's radar without being overly sensitive. Under the agreement, the wireless devices and radar will share the spectrum but the devices will be designed to jump to another frequency when they sense radar operating in their range. The time pressure was exerted by an approaching World Radio Conference, a biennial meeting under the aegis of the United Nations at which international spectrum allocations are ironed out. While the conference does not take place until June, the United States needs several months to lobby other nations to share its position. Despite the worldwide influence of both the United States military and technology companies, each nation has a single vote at the conference.

Source: <http://www.nytimes.com/2003/02/01/technology/01SPEC.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: 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), 1434 (ms-sql-m), 80 (http), 1433 (ms-sql-s), 53 (domain), 21 (ftp), 139 (netbios-ssn), 445 (microsoft-ds), 135 (???), 4662 (???) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

23. *February 03, New York Times* — **Key Indonesian terror suspect held.** The Indonesian police have arrested one of the most hunted terrorist suspects in Southeast Asia, Mas Selamat bin Kastari, who is accused of having been involved in plots to attack United States facilities in the region. **Kastari was arrested on Sunday, on the Indonesian island of Bintang, just off Singapore, the Indonesian police announced today. Singaporean authorities have said that Kastari is the leader of the Singaporean cell of Jemaah Islamiyah, the radical Islamic group based in Indonesia. Kastari had been on the run since December 2001, after a plot to blow up the American Embassy in Singapore was uncovered, and more than a dozen of Kastari's alleged cell members were arrested. He had threatened to retaliate by hijacking an American jet and crashing it into Singapore's airport.** In a white paper issued last month on Jemaah Islamiyah, and the threat of terrorism, the Singaporean government listed Kastari as one of the key people to be arrested, along with Riudan Isammudin, better known as Hambali. He remains at large. **Kastari's arrest is the latest in a crackdown on terrorism by the Indonesian government, which had long denied that terrorism was a threat here.**
Source: http://www.nytimes.com/2003/02/03/international/asia/03CND_I_NDO2.html

24. *February 03, Associated Press* — **Greece arrests three suspects in a drive against terror.** The Greek police arrested three suspected members of a radical far-left group in raids over the weekend, including the mayor of an Aegean island, the authorities said today. **The raids were part of a major police antiterror effort ahead of the 2004 Olympic Games in Athens.** The suspects, arrested on Saturday and today, were identified as Angeletos Kanas, 52, the mayor of the island of Kimolos; Constantine Agapiou, 56, a civil engineer; and Irene Athanasaki, 49. Kimolos is 95 miles southwest of Athens. **A police spokesman, Lefteris Economou, said the three were accused of taking part in a terrorist group, the Revolutionary Popular Struggle, which had eluded the authorities since it first appeared in 1975.** The suspects were being questioned at police headquarters here and were to appear before a public prosecutor. The police also questioned more than a dozen other people, none of whom were held.
Source: http://www.nytimes.com/2003/02/03/international/europe/03GRE_E.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.