



National Infrastructure Protection Center NIPC Daily Open Source Report for 28 February 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- USA TODAY reports top federal officials conclude that it would be easier than previously believed for enemies of the United States to build nuclear weapons using spent nuclear fuel, the waste generated by reactors. (See item [4](#))
- The Associated Press reports Baltimore city officials announced that at least 30 million gallons of raw sewage poured into a local waterway as a result of a blockage in a 3-foot-wide pipe. (See item [24](#))
- ZDNet reports United States-based security company @stake has released a security advisory detailing a Denial of Service vulnerability in the Nokia 6210 GSM mobile phone. (See item [34](#))
- Attorney General John Ashcroft in consultation with the Homeland Security Council decided today to return the national threat level to an elevated level of terrorist attack, or “yellow”. The joint statement of Attorney General John Ashcroft and Secretary of Homeland Security Tom Ridge explaining this decision can be found at http://www.usdoj.gov/opa/pr/2003/February/03_ag_122.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 27, Associated Press* — N. Korea restarts reactor, U.S. reports. Defying the Bush administration, North Korea has restarted a reactor at its main nuclear complex, possibly

laying the groundwork for additional atomic weapons beyond the one or two it is believed to possess already, U.S. officials say. The disclosure Wednesday was a blow to the administration's reliance on diplomatic pressure to induce the North to set aside its nuclear ambitions. The U.S. officials, asking not to be identified, said the reactivated facility starts a process that could yield nuclear weapons in about a year. **But Pyongyang could add to its supply much earlier if it restarts a processing plant adjacent to the reactor. The plant could be used to reprocess 8,000 plutonium-laden spent fuel rods at the site; there is enough plutonium there to build five or six bombs in a few months.** North Korea insists that its nuclear programs are designed entirely for peaceful purposes, a claim that U.S. officials and private experts reject.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A9143-2003Feb27.html>

- 2. February 27, Reuters — Philippine troops pursue rebels after blackout.** The Philippines said Thursday **Islamic militants using mortars blew up a power pylon, cutting power to almost all of the country's main southern island of Mindanao.** A loud explosion toppled the pylon in Lanao del Norte province late on Wednesday, plunging into darkness around 90 percent of the island's 24 million people. It was the 12th electrical transmitter operated by state-run National Power Corp to be disabled in the past two weeks in the wake of clashes between soldiers and the MILF, the biggest group fighting for an Islamic state in the south of the mainly Roman Catholic country. An army official said three mortar shells were used in the attack and troops were hunting for fighters from the Moro Islamic Liberation Front (MILF). The attack occurred as 60,000 troops were on high alert on the island to ward off what the military said were possible attacks by MILF guerrillas. **One of the cities affected by the outage was Zamboanga, where about 200 U.S. troops are training local soldiers in counter terrorism tactics to fight Muslim radicals.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A8826-2003Feb27.html>

- 3. February 27, Platts Global Energy News — OPEC producing more oil than market requires. World oil markets are not currently under-supplied, and OPEC is producing more than enough to satisfy demand, OPEC secretary-general Alvaro Silva said Thursday.** The market is "well served with oil," Silva told reporters at a monthly briefing at the cartel's Vienna headquarters. "We are producing more than our ceiling and more than the world is requiring, more than the demand of the world," he said. Current high prices were due to "concern about war," he said, adding OPEC had put an additional 2.8-mil b/d on the market since December. Silva said this increase was "more than real. **We have been producing our ceiling and more than that.**" NYMEX crude futures broke above \$38/bbl in out-of-hours trading Wednesday as the U.S. Department of Energy reported further falls in crude and heating oil stocks.

Source: <http://www.platts.com/stories/oil2.html>

- 4. February 27, USA TODAY — Fuel for nuclear weapons is more widely available.** U.S. officials have insisted for a decade that getting plutonium or highly enriched uranium is the big hurdle for rogue states or terrorists trying to build nuclear weapons. But for much of that time, they've known a secret: Other materials can be used to make atomic bombs, and they're a lot easier to get. **Classified nuclear threat reports warn that rogue countries and terrorists have learned it is possible to make atomic bombs using low-enriched uranium, a common fuel for nuclear reactors used to conduct research and generate power.** The reports,

described to USA TODAY by top federal officials, also conclude that it would be easier than previously believed for enemies of the United States to make such weapons using spent nuclear fuel, the waste generated by reactors. **Neither of those substances is listed as "weapons usable" under U.S. or international security protocols. As a result, they get little protection from theft at civilian nuclear reactors worldwide. That includes reactors in former Soviet states and nations such as Indonesia, where public sympathy runs high for Iraq and al Qaeda.**

Source: http://www.usatoday.com/news/world/2003-02-26-nuke-threat-co ver_x.htm

5. *February 26, Associated Press* — **Nuclear plant declares low-level emergency . The Kewaunee Wisconsin nuclear plant (near Green Bay) lost the use of both backup generators for several hours early Wednesday, prompting officials to declare a low-level emergency. There was no risk to public safety, they said.** Plant operators began a controlled shutdown shortly after midnight when one diesel generator failed to start during a daily test, according to the Nuclear Management Co., which runs the plant. The second backup generator was out of service for scheduled maintenance. **The incident was classified as an "unusual event," which is the lowest of the four emergency classifications established by the Nuclear Regulatory Commission for nuclear power plants.**

Source: <http://www.cnn.com/2003/US/Midwest/02/26/nuclear.plant.ap/index.html>

6. *February 26, Chattanooga Times/Free Press* — **Tennessee Valley Public Power Association opposes electricity rate increase .** Tennessee Valley Authority distributors are balking at higher electricity prices, claiming the federal utility has yet to demonstrate a need to raise and reallocate its rates. **Directors of the Tennessee Valley Public Power Association, who met with Tennessee Valley Authority (TVA) officials Tuesday, have adopted a resolution opposing a TVA plan to raise residential and commercial power rates while cutting industrial rates.** "We don't feel like we have been provided enough information yet about TVA's spending plans and we're concerned about the impact a rate increase of this size will have on our customers," said Richard Crawford, president of the Chattanooga-based trade group for TVA's 158 distributors. TVA Chairman Glenn McCullough Jr., said Tuesday he understands the concerns of his customers. McCullough, who heads the three-member TVA board, said the utility needs to raise rates this fall to cover unanticipated expenses of installing required pollution controls on most of its 11 coal plants across the Tennessee Valley. TVA plans to spend \$537 million this year on equipment to meet new federal limits on sulfur dioxide and nitrogen dioxide pollution. **By the end of the decade, TVA will have invested more than \$5 billion in cleaning up its aging coal plants. The utility could face billions of dollars of additional expenses if it is required to make further pollution controls, including possible new limits on mercury and carbon dioxide emissions, according to TVA President O.J. "Ike" Zeringue.** TVA is proposing to raise its wholesale rates to distributors on Oct. 1 by 8.1 percent for residential and commercial customers. At the same time, TVA wants to cut industrial rates by 2 percent.

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3674570

7. *February 26, Tennessee Valley Authority* — **TVA boosts commitment to renewable energy . The Tennessee Valley Authority (TVA) has signed a 20-year contract with Invenergy LLC, a Chicago-based energy-development company, to build and operate 18 power-generating windmills atop a mountain in eastern Tennessee. The new units will**

increase by 10–fold the amount of power generated by TVA's latest venture into renewable energy sources. **They'll join three windmills that have been operating on Buffalo Mountain, near Knoxville, for three years.**

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=cahners_2003_02_26_eng-cahners_eng-cahners_102639_2343035696948299349a>

8. *February 25, The Augusta Chronicle (Georgia)* — **Federal Report details plans for nuclear fuel facility in South Carolina.** A much–anticipated Nuclear Regulatory Commission report on a proposed Savannah River Site project (near Aiken, SC) has been released. **The draft report, called an environmental impact statement, details new elements of the Department of Energy plan to construct and operate a mixed–oxide fuel (MOX) fabrication facility at the site. The plant would convert weapons–grade plutonium into a form usable by commercial nuclear power plants for energy generation.** Under federal law, the public must be allowed to weigh in on the plant's potential effects on humans and the environment. Plans for MOX were developed under the Clinton administration as a peace agreement between United States and Russia. Each country pledged to rid itself of 34 metric tons of weapons plutonium.

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3673764

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

9. *February 27, Associated Press* — **Thirty–seven alleged illegal immigrants arrested. Thirty–seven people accused of being illegal immigrants were arrested at F.E. Warren Air Force Base, headquarters of the nation's largest arsenal of intercontinental nuclear missiles.** Forty–four employees of a U.S. Army Corps of Engineers subcontractor were originally arrested Wednesday. Seven later provided documents showing they were in the country legally, officials said. The other 37 "were taken into custody and they remain in our custody awaiting further investigation," INS spokeswoman Nina Pruneda said Thursday. **Immigration and Naturalization Service officials were trying to determine whether the aliens had access to secure areas. However, authorities do not believe any were linked to terrorists.**

Source: <http://wtopnews.com/index.php?nid=104ont>>

10. *February 26, Government Computer News* — **DoD prepares bandwidth RFP.** The Defense Information Systems Agency will issue a request for proposals within two weeks on the Global Information Grid–Bandwidth Expansion program, according to Defense Department officials. **A presolicitation notice for GIG–BE was released last week. The RFP, which could come as early as Friday, is for the acquisition of fiber to support the GIG–BE network, a**

worldwide, ground-based voice, data and imagery network with 10-Gbps OC-192 connections. DISA could select up to nine separate contractors or combine all of the requirements for GIG-BE under a single award. Either way, GIG-BE will provide an answer to the long-running problem of insufficient and poorly managed bandwidth that continues to plague Defense, said Air Force Major Gen. Charlie Croom Jr., who spoke on Wednesday during the TeleStrategies Conference in Vienna, VA.

Source: http://www.gcn.com/vol1_no1/daily-updates/21264-1.html

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

Banking and Finance Sector

11. *February 27, Wired* — **Credit card companies take care of themselves.** The credit card industry focuses too much on reducing its own fraud costs and not enough on protecting consumers. That's the central claim in a new report from research firm Gartner that discredits credit card companies for failing to notify consumers when credit card records are compromised by malicious hackers. **The report notes that while credit card companies' "zero-liability" policies protect card holders from paying for unauthorized or fraudulent charges, they do not protect consumers from identity theft and the credit report hell that can follow.** Avivah Litan, Gartner vice president and the report's co-author, said when security breaches happen, banks that issue credit cards seldom notify consumers. "The issuers claim they don't really know if a card was compromised after a merchant or transaction processing firm reports a problem, so they wait to see whether a consumer reports fraud against his or her card," Litan said. **"Of course the fact that closing potentially compromised accounts and providing consumers with new cards costs the issuer about \$35 per card is also a factor here. So the card issuers take a calculated risk that compromised cards won't be used fraudulently."** On Feb. 18, Visa, MasterCard and American Express confirmed that a malicious hacker had gotten access to 8 million credit card records through Data Processors International, a company that processes credit card transactions for mail order and online businesses. **According to Litan, the card issuers have tagged the accounts believed to have been compromised in the theft, and will watch them for a period of time, typically three to six months, for possible fraudulent use.** Report Summary: http://www3.gartner.com/DisplayDocument?doc_cd=113282
Source: <http://www.wired.com/news/privacy/0,1848,57823,00.html>

12. *February 26, Reuters* — **House backs wider emergency powers for SEC.** The U.S. House of Representatives on Wednesday approved a bill to give the Securities and Exchange Commission more power over the markets in case of another emergency like the Sept. 11, 2001, attacks. **The SEC could take wider and longer-lasting control of markets in emergencies under the bill, closely resembling one the House passed in 2001, but the Senate never cleared. The bill would let the SEC issue emergency orders for up to 90 days in case of "sudden and excessive fluctuations of securities prices," disruption of transaction systems or in other urgent circumstances.** It would also broaden the SEC's emergency jurisdiction over more sections of securities law, with some consultation required with the Treasury Department, the Commodity Futures Trading Commission and the Federal Reserve Board. **The SEC's emergency decree powers are now limited to 10 days. They were last invoked after the Sept. 11 attacks.**

Source: CRS Summary:

<http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR00657:@@@Dmm2=mStory>:

http://story.news.yahoo.com/news?tmpl=story1_nm/congress_sec_emergency_dc_1

[[Return to top](#)]

Transportation Sector

13. *February 27, Australian IT* — **Face recognition fails test.** The much-heralded SmartGate facial recognition trial at Australia's Sydney Airport has suffered an embarrassing setback, with two Japanese visitors fooling the system simply by swapping passports. **The automated system, which is a world-first attempt at using photo-matching technology for border control, falsely identified both men as matching the images contained in each other's travel documents.** SmartGate is intended to replace the identity check performed by Customs officers and is supposed to take into account differences such as age and ethnicity and variations due to hairstyles or glasses. The men were attending a demonstration along with other international members of IATA's Simplifying Passenger Travel committee meeting in Sydney this week. Minister for Customs Chris Ellison has confirmed that two Japanese participants were falsely accepted as each other. "At the time, SmartGate was in demonstration mode and the men were not subject to all the security checks incorporated within the system," he said.

Source: http://www.news.com.au/common/story_page/0,4057,6048331%25E15306,00.html

14. *February 26, Government Executive* — **TSA looks beyond aviation security.** When the Transportation Security Administration moves over to the Homeland Security Department March 1, it will need to demonstrate that it can effectively coordinate security for all modes of transportation, not just aviation. Since its inception a little over a year ago, TSA has been almost entirely focused on air travel. To be sure, the agency was under tight congressional deadlines to hire tens of thousands of passenger and baggage screeners. **Having met those deadlines, the agency must now turn its attention to other modes of transportation. To that end, the TSA is working on a national security plan that will address all modes of transportation,** according to TSA Administrator James Loy. **Part of that plan will call for partnerships with the private sector. TSA must reach out to various industry groups to develop new security protocols,** Loy said at a press conference on Wednesday. **TSA is drafting memorandums of understanding with various Transportation agencies to determine how they will coordinate work in the future.** The agreements, he said, are a way to assure Transportation officials that the collaboration will continue. At the same time, they are a sign to Homeland Security Secretary Tom Ridge that, as Loy said, "he has important customers at Transportation."

Source: <http://www.govexec.com/dailyfed/0203/022603w1.htm>

15. *February 26, Federal Computer Week* — **TSA prepares passenger screening system. The Transportation Security Administration next month plans to begin testing a computer system that will perform background checks and risk assessments on airline travelers.** Delta Air Lines and IBM Corp. are collaborating with TSA on the preliminary stages of a pilot project for the Computer Assisted Passenger Pre-Screening II program, called CAPPS II. Passengers will activate CAPPS II when they make flight reservations, with their travel

information passing from airlines to TSA. **The agency will then run individual searches, scanning government and commercial databases for data that could indicate a potential threat. Based on its findings, the agency will assign a red, yellow or green score to travelers, ultimately appearing on their boarding passes.** The determination for red — a branding that prevents the passenger from flying — will rest on a watch list, compiled by the intelligence and law enforcement authorities, officials said. Passengers branded in the yellow category, meanwhile, will face additional screening before being allowed to board. "Green" passengers will be free to go, officials said. **CAPPS II could eventually spawn the Registered Traveler Program, which will allow certain credentialed and pre-screened passengers to speed through security checkpoints in airports.**

Source: <http://www.fcw.com/fcw/articles/2003/0224/web-tsa-02-26-03.a.sp>

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

Postal and Shipping Sector

16. *February 27, South China Morning Post* — **China poised to sign U.S. accord on tighter cargo security. Authorities on the mainland are close to signing the same global security agreement which next month will see United States Customs Service agents patrolling Hong Kong's docks for potential terrorist shipments.** On Wednesday, Deputy U.S. Customs Commissioner Douglas Browning described discussions on gaining China's acceptance of the Container Security Initiative (CSI) as "very healthy", and tipped the deal would be signed soon. "We are close to what we think may be **the final draft on the declaration of principle and we are hopeful of getting [the CSI] done by early summer at the latest,**" Browning told the Terminal Operating Conference 2003 at the Hong Kong Convention and Exhibition Centre. U.S. Customs officials are already in place at ports in Canada and several cities in Europe and Browning said the department was planning to have agents in Hong Kong, Singapore and Yokohama by the end of next month. **When China signs, phase one of the CSI, which involved gaining co-operation from the top 20 "megaports" exporting to the U.S., will have been completed.**

Source: <http://www.scmp.com/topnews/ZZZD1WR4JCD.html>

17. *February 27, Federal Register* — **Coast Guard issues a temporary final rule establishing security zones in the San Francisco Bay, CA. The Coast Guard is establishing moving and fixed security zones extending 100 yards around and under all High Interest Vessels (HIVs) that enter, are moored in, anchored in or depart from the San Francisco Bay and Delta ports, California. These security zones are needed for national security reasons to protect the public and ports from potential subversive acts.** Entry into these security zones is prohibited, unless specifically authorized by the Captain of the Port San Francisco Bay, or his designated representative. This regulation is effective from 11:59 p.m. PST on February 10, 2003 to 11:59 p.m. PST on May 31, 2003.

Source: <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-4634.htm>

18. *February 25, MSNBC* — **Coast Guard is still sailing blind.** Nearly 18 months after the Sept. 11 terror attacks and despite repeated warnings of the threat to American ports, **U.S. officials still have no way of identifying the hundreds of cargo ships currently plying U.S. coastal**

waters. Critics say efforts to fix the problem have been bogged down in resistance from shippers, with a solution still a year and a half away. "What bothers me is I still see inaction," said Capt. Ed Page, former Coast Guard captain of the Port of Los Angeles–Long Beach and now vice president of the Maritime Information Services of North America, a non–profit group of maritime–related companies. **The MISNA group wants all large cargo vessels equipped with gear that would use an Inmarsat satellite to automatically tell security officials the ship's name, course, speed and location.** But so far the International Maritime Organization (IMO), which regulates international shipping, is not willing to go along. **Instead, in a new directive published in January, the IMO is giving ship owners until the end of next year, 2004, to install a short–range system that will identify ships within 20 to 25 miles of the U.S. coast — but not in the open ocean.** Whether the broader system — similar to that used to track commercial airliners — will ever be adopted is still in doubt. "The intelligence community would like to have that capability," said Anthony Regalbuto, former acting director of port security for the Coast Guard and now head of the agency's office of policy and planning for port security. **Some shippers are worried that competitors could use the satellite data to their advantage; others argue that terrorists themselves could abuse the system to find their targets.**

Source: <http://www.msnbc.com/news/877139.asp>

[[Return to top](#)]

Agriculture Sector

19. *February 27, Associated Press* — **Wisconsin wasting disease plan draws fire. A \$1 billion hunting industry remains in jeopardy because Wisconsin after spending more than \$12 million is still learning how far chronic wasting disease has spread into the herd, and has no idea how it got to the area in the first place.** Many hunters and landowners have refused to participate in the state's strategy to wipe out the disease killing all deer in the infected area. Consequently, officials are forced to rely on government sharpshooters to reduce the herd. "I would argue their response to this thing is wounding hunting in Wisconsin more than the problem itself," farmer and hunter Mark Peck said of the state's strategy. **So far, about 8,000 deer have been killed near Mount Horeb in the eradication zone barely one year's fawn crop.** Some landowners even signed petitions pledging not to help the state reduce the number of deer in the area, contending it's impossible to kill all the deer, and saying the plan puts an unfair and unreasonable burden on them. **Governor Jim Doyle said it might be time for a new approach to deal with a disease.**

Source: http://abcnews.go.com/wire/US/ap20030227_341.html

20. *February 27, Associated Press* — **Health officials shut down oyster beds after bacteria risk rises. Alabama health officials closed all the oyster beds in Mobile and Baldwin counties to harvesting because of a high risk of bacterial contamination.** Officials closed the beds on Wednesday afternoon, saying the risk increased after a flow of upland freshwater into Mobile Bay from recent rains. Included in the closings were Cedar Point, Portersville Bay, Grand Bay, Heron Bay, Dauphin Island Bay, and Bon Secour Bay. "This is bad news for a lot of people right now," said Avery Bates, a lifelong Bayou La Batre oysterman. **"With the shrimp market bottomed out, we've had all those men out on the reefs tonging to get by. Now they can't even do that."**

Source: http://www.al.com/newsflash/regional/index.ssf?/newsflash/get_story.ssf?cgi-free/getstory_ssf.cgi?j5898_BC_AL-BRF--OysterBedsal

21. *February 27, Sarasota Herald Tribune* — **Canker quarantine expanded. Florida's agriculture commissioner on Wednesday established three new canker zones in Sarasota, Manatee, and Lee counties as part of a years-long struggle against the citrus disease.**

Citrus growers in quarantine zones are forced to adhere to strict decontamination procedures and barred from selling fruit to other citrus-growing states. Canker can weaken citrus trees and cause fruit to fall prematurely. The disease can be costly to Florida's \$9 billion citrus industry. Florida Department of Agriculture and Consumer Affairs spokeswoman Denise Feiber said legal challenges to the canker eradication efforts hampered the state from designating the new canker zones.

Source: <http://www.heraldtribune.com/apps/pbcs.dll/article?Site=SHD&ate=20030227&No=302270769007>

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

Food Sector

22. *February 27, Georgia Institute of Technology* — **Researchers design system to improve disinfection of water used in food processing. Georgia Institute of Technology researchers have developed a better-performing, less costly method of disinfecting water used in food processing.** Like current technologies, the new Advanced Disinfection Technology System relies on ultraviolet (UV) radiation to eliminate molds, viruses, and bacteria. But the new system handles water more efficiently and thus improves the overall effectiveness of the disinfection process, researchers reported. "We're creating a mixing pattern to ensure that every particle of water is equally exposed to the UV lamp," said John Pierson, a senior research engineer at the Georgia Tech Research Institute and co-principal investigator. "By doing a better job of mixing the water, you get better disinfection." **Federal regulations require the disinfection of water used in food processing before it can be reused. In many cases, the lack of cost-effective disinfection means water is used only once and then discarded.**

Source: <http://www.sciencedaily.com/releases/2003/02/030227073942.htm>

23. *February 27, Edinburgh Evening News* — **Scientists find source of E. coli. Scientists at Edinburgh University, in Scotland, have identified the source of the potentially fatal E-coli 0157 bacterium in cattle for the first time. It is hoped the discovery will eventually help to remove the organism from the food chain.** E. coli is common in cattle and sheep and is spread to humans either by direct or indirect contact with animal feces. Until now, it was not known where the bug colonised in the gastrointestinal tract of cattle. But veterinary microbiologists at Edinburgh University have found the majority of the bacteria can be found just inside the animal's rectum. The breakthrough came after the discovery of a different cell type lining the gastrointestinal tract. Dr David Gally, one of the scientists involved in the research project, said there was now a strong possibility the presence of E. coli could be "eradicated" from the food chain. **"This knowledge gives us the potential to identify, control, and ultimately eradicate E. coli 0157 in the minority of livestock that are carriers of the bacterium,"** he said.

Source: <http://www.edinburghnews.com/index.cfm?id=244972003>

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

Water Sector

24. *February 27, Associated Press* — **Blocked pipe blamed for 30 million gallon sewage spill in Baltimore. At least 30 million gallons of raw sewage poured into Herring Run in Baltimore, MD. The result of a blockage in a 3-foot-wide pipe, city officials said.** Health warnings were posted Wednesday along parts of a 6-mile stretch of the waterway, which flows into the Back River near Essex. "This may be the biggest one in my 10 years," Dr. Peter L. Beilenson, the city health commissioner, said. The spill is enough to fill 45 public swimming pools. A passer-by discovered the backup on Monday and notified the Herring Run Watershed Association. The association then alerted the city Department of Public Works. **After determining the magnitude of the spill, public works officials notified the city Health Department on Wednesday morning, which then posted warnings to avoid contact with the water. The signs will stay posted until the water tests safely.**

Source: <http://wtopnews.com/index.php?nid=25ont>>

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

Public Health Sector

25. *February 27, Herald* — **Solution to the superbug may lie in rock pool. An antibiotic that kills Methicillin Resistant Staphylococcus Aureus (MRSA) has been discovered by scientists in slime taken from rock pools.** "It appears to be very potent in terms of what concentration is required to kill MRSA," said Dr Jonathan David, who led a team of researchers along Scotland's coastline hunting for samples. "It completely stops them dead, preventing any further growth and killing the existing bacteria," he said. Several types of bacteria found by the five-person team from Edinburgh produce an antibiotic that acts against the bug responsible for doubling the death rate from staphylococcal infections in the UK between 1993 and 1998. Health services are fighting a losing battle against MRSA, which is impervious to most antibiotics and poses the greatest threat to patients who have undergone surgery. **Researchers said the new antibiotic was so effective it has already attracted keen interest from the big drug companies.**

Source: <http://www.theherald.co.uk/news/archive/27-2-19103-0-10-39.html>

26. *February 27, Associated Press* — **Experiment planned in Fort Lauderdale to use pest killer on anthrax. Environmental officials and a Florida lawmaker will be closely watching a planned experiment to test a pest-killing gas as a possible way to eliminate anthrax spores from a tabloid publisher's former office building.** A test scheduled for Friday in a Davie trailer will use methyl bromide gas on harmless bacteria used as a stand-in for anthrax spores. **University of Florida entomologist Rudolph Scheffrahn and his partner, Mark Weinberg, a Lauderhill exterminator, contend the chemical could be used to clean the offices of the contaminated American Media Inc (AMI) building in Boca Raton for \$2 million. Estimated cleanup costs currently range from \$7 million to \$20 million.** The AMI building has been quarantined since anthrax killed Sun photo editor Robert Stevens in October 2001.

Source: http://www.heraldtribune.com/apps/pbcs.dll/article?Date=2003_0227No=302270625>

27. *February 27, Oakland Tribune* — **Biodefense can have everyday use, too, scientists say.**

Lured by a new, biodefense market estimated to be worth billions of dollars, biotech executives and investors on Wednesday listened eagerly, if cautiously, as scientists talked of an even larger potential industry making chemical and biological sensors for everyday living. **The high-tech tools for guarding against terrorist attacks, scientists said, can do double duty as sniffers for natural germs in cities and hospitals, detecting the cause of sick buildings, and keeping foods safe from bacteria and insecticides.** "It can't just be for biodefense," said J. Patrick Fitch, manager of Chemical and Biological National Security Programs at Lawrence Livermore Laboratory. "Sustainability will have to come from having benefits aside and apart from these low-probability terrorist events."

Source: <http://www.oaklandtribune.com/Stories/0.1413.82~1865~1208276.00.html>

28. *February 25, Detroit Free Press* — **U.S. coughs up billions to combat the common cold. The common cold costs the U.S. economy \$40 billion a year in treatments and lost workdays, according to a new study by the University of Michigan that appears to be the first to quantify the cost of the most commonly occurring illness in humans.** Researchers were not surprised to learn there are approximately 500 million colds each year in the United States. What was surprising, says Dr. A. Mark Fendrick, lead author of the study released Monday, "Was how often the public uses the health system to treat a cold." **Based on a nationwide phone survey of more than 4,000 households, researchers found that cold sufferers visit the doctor more than 100 million times each year at a cost of at least \$7.7 billion, Fendrick said.** The biggest economic cost was in lost workdays, something people tend not to consider when weighing the cost of illness, Fendrick said. **He and his team estimated that parents miss an average of 126 million workdays to care for their sick children. They miss 70 million more because they are sick. This costs the U.S. economy \$22.5 billion a year.**

Source: http://www.freep.com/money/business/cold25_20030225.htm

[[Return to top](#)]

Government Sector

29. *February 27, New York Times* — **White House concedes that counterterror budget is meager.** Responding to criticism from Democrats and to the mounting concern of state and local governments, the White House is now saying that the long delayed government spending plan for the year does not provide enough money to protect against terrorist attacks on American soil. In a speech on Wednesday to the National Governors Association, President Bush referred to the \$3.5 billion that the White House requested more than a year ago for state and local governments to pay for counterterrorism equipment and training, a centerpiece of the administration's domestic security program. **White House officials say they believe the \$397.4 billion spending bill, which will finance the government through September, contains only about \$1.3 billion in counterterrorism money for local governments, with most of that money going to emergency-response programs that had little to do with counterterrorism, a view shared by some private budget specialists who have reviewed the bill.**

Source: <http://www.nytimes.com/2003/02/27/politics/27HOME.html>

30. *February 27, U.S. Department of Homeland Security* — **Attorney General John Ashcroft and Secretary of Homeland Security Tom Ridge jointly announce lowering of threat level.** Based on a review of intelligence and an assessment of threats by the intelligence community, the **Attorney General in consultation with the Homeland Security Council has made the decision to return the threat level to an elevated risk of terrorist attack, or "yellow" level.** The decision to raise the threat level on February 7 was based on specific intelligence, corroborated by multiple intelligence sources, received and analyzed by the full intelligence community at the time. Today's decision to lower the threat level was based on a careful review of how this specific intelligence has evolved and progressed over the past three weeks, as well as counter-terrorism actions the U.S. government has taken to address specific aspects of the threat situation. **Among the factors considered was the passing of the time period in or around the end of the Hajj, a Muslim religious period ending mid-February 2003. The lowering of the threat level is not a signal to government, law enforcement or citizens that the danger of a terrorist attack is passed. Returning to the elevated level of risk is only an indication that some of the extra protective measures enacted by government and the private sector may be reduced at this time.**

Source: <http://www.dhs.gov/dhspublic/display?theme=87/font>>

31. *February 26, Government Executive* — **State, local officials seek better info from feds on terrorist threats.** State and local officials have been frustrated by the "imprecise and inadequate" information on terrorist threats they receive from the CIA, FBI and other federal agencies, several homeland security officials said on Wednesday. "They don't feel like they have all the cards in the deck that we have," John Pistole, the FBI's deputy assistant director for counterterrorism, said during a conference sponsored by the Armed Forces Communications and Electronics Association. **Pistole said state and local officials have sought more frequent and thorough intelligence analyses from federal agencies about "where we are in the entire threat arena." Although it is "very rare" for intelligence agencies to obtain information about specific terrorist targets, according to John Gannon, a former chairman of the National Intelligence Council, they must provide state and local officials with better information about how the threat-alert level might affect their communities.** Gannon added that the increased threat level is impacting state and local budgets "in a very significant way" because even if officials perceive a low risk of the threat affecting their regions, such alerts will prompt a public demand for increased police protection. **Intelligence and law enforcement officials on the panel said they are working to improve communications with state and local agencies. For example, the CIA hopes to create "profiles" of authorized intelligence recipients throughout the country and disseminate information on a targeted basis, according to William Dawson, deputy chief information officer for the CIA's intelligence community office.**

Source: <http://www.govexec.com/dailyfed/0203/022603td1.htm>

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

Emergency Services Sector

32. *February 27, Associated Press* — **FEMA 9/11 tally has \$260M for pensions.** A final tally of the \$8.8 billion in federal emergency funds for New York's post-Sept. 11 recovery includes

\$260 million to help pay pension benefits to the families of firefighters and police officers killed in the attacks. **The accounting released Wednesday by the Federal Emergency Management Agency details \$2.4 billion for debris removal and related work, \$500 million for services and counseling to victims and their families, and nearly \$3.2 billion to rebuild transportation and infrastructure. The \$8.8 billion is part of more than \$20 billion President Bush has pledged for New York.** The survivors of rescue workers killed in the collapse of the World Trade Center towers are entitled to full pensions, and FEMA said Wednesday it would contribute \$260 million to help pay those costs.

Source: http://www.washingtonpost.com/wp-dyn/articles/A7478-2003Feb2_6.html

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

Information and Telecommunications Sector

33. *February 27, The Washington Times* — **Anti-war 'virtual march' jams Hill circuits.** An anti-war "virtual march" yesterday aimed at Capitol Hill led to a deluge of phone calls to some lawmakers' offices but barely had an effect on others. Although organizers of the Virtual March on Washington said 120,000 people had registered with the anti-war Web site www.moveon.org to call Capitol Hill, some offices there reported only moderately more traffic than usual. Others, such as the office of Sen. Dianne Feinstein, California Democrat, had six operators answering continuously ringing lines. Most callers were polite, staffers said. A staff member for Sen. Sam Brownback, Kansas Republican, reported few college students but many elderly people on the lines. "A lot of the people were reading off scripts," he said, "and many of them were moms at home with their children."

Source: <http://www.washingtontimes.com/national/20030227-92610576.htm>

34. *February 26, ZDNet (Australia)* — **Experts say mobile phone hacking may spread.** United States-based security company @stake has released a security advisory detailing a Denial of Service (DoS) vulnerability in the Nokia 6210 GSM mobile phone. "This is a good example of why all newly introduced product functionality should be reviewed to ensure that no new security vulnerabilities will also be introduced. A cursory source code audit would find an error of this type," the advisory said. The vulnerability is not serious — affected users can simply "reboot" their phones — but it could be a sign of worse things to come. John Papandriopoulos, a wireless communications researcher based in Melbourne, Australia, says that current generation handsets are not necessarily a popular target because there's little that can be done even if an attacker is able to compromise them. "I think it's more likely that the motivation would be to inconvenience people," he said. As for a mobile phone worm, spreading by sending itself to phonebook entries, John says this isn't likely to happen for some time. However, as standardized client software becomes a standard feature on mobile handsets it's only a matter of time before malicious hackers start paying more attention to wireless worms, according to security consultant Daniel Lewkovitz of Sydney, Australia.

Source: http://www.zdnet.com.au/newstech/security/story/0.2000024985_20272408.00.htm

35. *February 26, Federal Computer Week* — **Info sharing hobbled by lack of technology.** Agencies merging into the Homeland Security Department as well as others sharing information in the government's antiterrorism efforts are working to overcome technological barriers, but the work is going to take time, according to a panel of agency

officials who spoke February 26 at an AFCEA International Inc. conference in Washington, D.C. **One challenge is ensuring that information stays out of the hands of those not authorized to see it.** To that end, **the National Security Agency (NSA) is developing "trusted control interfaces," which the CIA is implementing,** said William Dawson, chief information officer of the CIA's Department of Intelligence Communications. **The interfaces' intent is to strip classified information from messages before passing them to someone of a lower security class.** An early stage of the system is running at the CIA, but most of the capabilities won't be ready until September, Dawson said.

Source: <http://www.few.com/few/articles/2003/0224/web-info-02-26-03.asp>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.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), 1434 (ms-sql-m), 80 (www), 113 (ident), 4662 (eDonkey2000), 4665 (eDonkey2000), 4672 (---), 445 (microsoft-ds), 25 (smtp), 53 (domain) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

36. February 27, Seattle-Post Intelligencer — Anti-terror forces arrest Idaho student. Agents with a federal anti-terrorism task force on wednesday arrested a University of Idaho student who they say provides a window on how al Qaeda, the group responsible for the Sept. 11, 2001, attacks, raises money. **Sami Omar Al-Hussayen, a doctoral candidate studying computer security here, was a terrorist moneyman, according to one federal criminal justice source.** Al-Hussayen, who is from Saudi Arabia, had been a committed student leader at the University of Idaho, where he has studied since 1999. He once was president of the local chapter of the Muslim Students Association and gave blood after the Sept. 11 attacks, then marched with others in a peace rally. Al-Hussayen, 35, is married and the father of two children. The charges against Al-Hussayen involve immigration crimes with only tangential relationships to terrorism. **But investigators say the accusations do not reflect the central role that investigators believe Al-Hussayen has played in the flow of al Qaeda cash. Federal agents coordinated the 4 a.m. arrest of Al-Hussayen in this quiet college town of 18,000 people**

with the arrests of four Arab men around Syracuse, N.Y., and searches of a Muslim charity operation in greater Detroit.

Source: http://seattlepi.nwsourc.com/local/110332_terrorists27.shtm 1

37. *February 27, Associated Press* — **Cyanide attack threatened if war in Iraq.** In terror threats sent to the U.S., Australian and British embassies in New Zealand, **a group calling itself "September 11" claimed it had 55 pounds of cyanide it will use against the America's Cup yacht race and U.S. interests if Iraq is attacked,** police said Thursday. Although the group's name referred to the 2001 attacks in the United States by the al-Qaeda network, national police headquarters spokesman John Neilson said **police believed the threat came from within New Zealand. "Certainly there has been no suggestion at this point of any links to any other organization, including international terrorist groups,"** he said. A squad of anti-terror police was working to find the author of the four identical letters, which specifically mentioned the America's Cup yacht race in Auckland. The letters, written in English littered with grammatical and spelling errors, said: "September 11 waits at the Americas Cup for instruction if Iraq is attacked by the host of satan all interests and there supporters will be attacked by September 11...**September has stockpiled 25 kilo (about 55 pounds) weapon grade cyanide and will use those against those interests wherever they are,**" the threat adds.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A9071-2003Feb27.html>

38. *February 26, Associated Press* — **Sentencing postponed in 2000 bomb plot.** A federal judge postponed sentencing Wednesday for convicted terrorist Ahmed Ressay after being assured the defendant will be eligible for a shortened sentence in exchange for help he has provided in terror investigations. **Federal prosecutors have persuaded U.S. District Judge John Coughenour to delay sentencing several times, citing fears Ressay would stop cooperating once he's handed a prison term. Since Ressay's conviction nearly two years ago in a foiled plot to blow up Los Angeles International Airport on Jan. 1, 2000, the Algerian national has given federal authorities information that has helped in several investigations.** Coughenour spoke highly of Ressay's contributions at Wednesday's hearing. "Everything I've seen and heard to date confirms in my mind that Ressay is now trying to do the right thing and has given rather startlingly helpful information to the government," the judge said. Sentencing had been scheduled for March 13. Coughenour did not set a new date but scheduled a status conference on sentencing for Oct. 1.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A8245-2003Feb26.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 Warnings](#) – NIPC Assessments, Advisories, and Alerts: The NIPC produces three levels of infrastructure warnings which are developed and distributed consistent with the FBI's National

Threat Warning System. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

[NIPC Publications](#) – NIPC Daily Reports, CyberNotes, Information Bulletins, and other publications

[NIPC Daily Reports Archive](#) – Access past NIPC Daily Reports

NIPC Daily Open Source Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the NIPC Daily Report Team at 202-324-1129

Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact NIPC

To report any incidents or to request information from NIPC, contact the NIPC Watch at nipc.watch@fbi.gov or call 202-323-3204.

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.