



# National Infrastructure Protection Center

## NIPC Daily Open Source Report for 04 March 2003

Current Nationwide Threat Level is



[For info click here](#)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

### Daily Overview

- The Associated Press reports that for cruise ship passengers, Miami is screening bags at the port and sending them directly to the airport, thus reducing the likelihood that luggage could be tampered with while shortening security lines at the airport. (See item [8](#))
- The Boston Globe reports five in Boston were infected with a powerful, drug-resistant bacteria, similar to recent, larger outbreaks in Los Angeles and San Francisco. (See item [16](#))
- The National Infrastructure Protection Center has released Advisory 03-004: "Remote Sendmail Header Processing Vulnerability". (See item [23](#))
- The National Infrastructure Protection Center had released Advisory 03-003: "Snort buffer overflow Vulnerability". (See item [24](#))
- Note from the Editor: The ISS AlertCON and Security Focus ThreatCon were changed from Level 1 to Level 2 yesterday. See the Internet Dashboard for details.

### 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. *March 03, Reuters* — **Three Wisconsin nukes to receive new reactor lids.** Two Wisconsin utilities plan to relace three reactor vessel heads at their nuclear power plants in the state at an overall cost of nearly \$64 million, plant operator Nuclear Management Co. said on Monday. **The plans stem from safety concerns raised at other U.S. nuclear power plants, where**

**cracks have been discovered in the heavy metal heads bolted onto the tops of the reactors.** Inspections, however, have not turned up any problems in the Wisconsin plants' vessel lids. **Rather, the utilities said it would cost them less to install new caps on the reactor vessels than face frequent inspections ordered by the U.S. Nuclear Regulatory Commission, which are running at \$6 million to \$7 million each.** Utility Wisconsin Public Service Corp., a unit of WPS Resources Corp. plans to replace the reactor vessel head on its Kewaunee nuclear power plant in autumn 2004 at an estimated cost of \$23.8 million. Wisconsin Energy Corp. plans to replace two vessel heads at its twin-unit Point Beach nuclear station in 2005 at a total cost of \$40 million, a spokeswoman for Nuclear Management told Reuters. The NRC has ordered inspections of all of the nation's pressurized water reactors to determine whether any vessel heads need to be replaced. **The inspections were ordered last year after FirstEnergy Corp. found cracks in the lid capping the reactor at its Davis-Besse plant in Ohio.**  
Source: [http://biz.yahoo.com/rc/030303/utilities\\_wisconsin\\_2.html](http://biz.yahoo.com/rc/030303/utilities_wisconsin_2.html)

2. *March 03, Boston Globe Online* — **Vermont Yankee operator eyes upgrade. Entergy Nuclear, which wants to increase the output from the Vermont Yankee nuclear power plant (near Battleboro, VT) by 20 percent, filed a letter of intent with the Vermont Public Service Board last week for approval of the \$60 million project, saying it would produce power at competitive rates.** The project would require construction and alteration at the 30-year-old plant, but not outside the plant's existing structure, according to an Entergy spokesman. The company has not yet applied to the federal Nuclear Regulatory Commission for approval for the power increase, though the utility hopes to start construction on the plant's cooling towers this fall, according to a letter filed with the state  
Source: [http://www.boston.com/dailyglobe2/062/metro/Vermont\\_Yankee\\_operator\\_eyes\\_upgrade+.shtml](http://www.boston.com/dailyglobe2/062/metro/Vermont_Yankee_operator_eyes_upgrade+.shtml)
3. *February 28, Las Vegas Review-Journal* — **Federal agency describes Nevada as favorable site for renewable power projects.** Nevada is identified in a new federal report as a "highly favorable" state to develop renewable energy on public lands. **The report, issued by the Bureau of Land Management, says Nevada tax law is favorable to investment. It also cites the state's renewable portfolio standard, which requires utilities to derive increasing percentages of their power supply from nonfossil sources.** In geothermal power, the BLM identified 10 sites in Nevada as holding high potential for "near term" energy development, including areas around Carson City, Elko, Battle Mountain and Winnemucca. Other tracts in the state were singled out for wind, solar and dispersed solar power, or photovoltaic, opportunities, the data, released last week by the BLM and the National Renewable Energy Laboratory, show. **At a Senate hearing Thursday, Interior Department official Steven Griles maintained alternative and renewable energy sources are critical components of President Bush's energy policy.**  
Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3681028](http://www.energycentral.com/sections/news/nw_article.cfm?id=3681028)
4. *February 28, BBC Monitoring Former Soviet Union* — **Ukraine nuclear monopoly slams chief over safety.** The supervisory board of the national nuclear power generating company, Enerhoatom, has requested the Ukrainian Cabinet of Ministers to take disciplinary action against Enerhoatom's president Serhiy Tulub in order to ensure that a stepped-up safety program is implemented at nuclear power plants. According to the decision, Enerhoatom's board of directors failed to implement a reactor upgrade program. In

2002, the company performed only 71 tasks, or 35.1 per cent, of those envisaged in the program. Also, the program was unsatisfactorily financed, despite the fact that funding outlays were incorporated in Enerhoatom's electricity rate and that payments made by the energy market to the company in September through December 2002 for electricity produced exceeded 100 per cent. **Under the supervisory board decision, Enerhoatom's board of directors must implement the program's priority areas, including stepping up operational safety at nuclear power plants as provided for in the electricity rate.**

Source: [http://www.energycentral.com/sections/news/nw\\_article.cfm?id=3681921](http://www.energycentral.com/sections/news/nw_article.cfm?id=3681921)

5. *February 28, UtiliPoint International* — **Alaskan pipeline may cross barriers.** The long cold winter has fired up debate over the Alaskan natural gas pipeline. **A combination of high gas prices coupled with dwindling supplies have sparked talks of compromise.** Divisions now exist over what route the pipeline would take as well as the level of U.S. government involvement. **Market pressures to bring the 35 trillion cubic feet (tcf) of known natural gas reserves in Alaska's North Slope are building.** The pipeline was originally authorized by the Federal Energy Regulatory Commission under the Alaska Natural Gas Transportation Act that went into effect July 1, 1979. Construction began soon after but stopped in the early 1980s, largely because of the availability of low-cost Canadian gas. Canadian objections have also kept the project at bay, mainly over what route the pipeline would take. Alaska wants the gas line to follow the oil pipeline down to Fairbanks, and then go eastward to Canada. This would assure that only Alaska gas gets transported through the line. **The Canadians fear that a pipeline from the north that does not include their Mackenzie region would leave them with “stranded” gas. They furthermore worry that American subsidies would make their gas less competitive.**

Source: [http://hsweb01.screamingmedia.com/PMA/pma\\_newsarticle1\\_national.htm?SMDOCID=UtiliPoint+International+2003+02+28+10464781+74354a](http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=UtiliPoint+International+2003+02+28+10464781+74354a)

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

## **Chemical Sector**

Nothing to report.

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

## **Defense Industrial Base Sector**

6. *March 03, Washington Times* — **Terrorists aim at Pearl Harbor.** Terrorists linked to al Qaeda have targeted U.S. military facilities in Pearl Harbor, including nuclear-powered submarines and ships, The Washington Times has learned. Intelligence reports about the terrorist threat to the Hawaiian harbor were sent to senior U.S. officials in the past two weeks and coincided with reports of the planning of a major attack by Osama bin Laden's terrorist group. **According to officials familiar with the reports, al Qaeda is planning an attack on Pearl Harbor because of its symbolic value and because its military facilities are open from the air. The attacks would be carried out by hijacked airliners from nearby Honolulu International Airport that would be flown into submarines or ships docked at Pearl Harbor in suicide missions, said officials who spoke on the condition of anonymity.**

**"The targeting includes nuclear ships and submarines and military facilities in the Pearl Harbor area," a defense official said.** The harbor is the home for 30 Navy and Coast Guard warships, including 18 nuclear submarines, five destroyers and two frigates. An additional terrorist target is said to be Hickam Air Force Base, located next to Honolulu airport and less than five miles from Pearl Harbor. Warplanes, transports and refueling tankers are based there. Source: <http://www.washingtontimes.com/national/20030303-104.htm>

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

## **Banking and Finance Sector**

- 7. *March 03, Department of the Treasury* — U.S. Treasury Department announces new executive office for terrorist financing and financial crimes.** The United States Treasury Department announced on Monday the formation of a new Executive Office for Terrorist Financing and Financial Crimes (EOTF/FC) reporting directly to the Deputy Secretary. This office has been charged with coordinating and leading the Treasury Department's multi-faceted efforts to combat terrorist financing and other financial crimes, both within the United States as well as abroad. The Office will work closely with other offices within the Treasury and throughout the U.S. government to identify, block, and dismantle sources of financial support for terror and other criminal activities, including money laundering. In addition, the team will work with international partners to expand the fight against terrorist financing and financial crimes in other nations. The Office will focus on reducing the risk that the domestic and international financial systems are being misused by criminals and terrorists. **The office will be led by Juan Zarate, Deputy Assistant Secretary for Terrorist Financing and Financial Crimes. Zarate will report to the Deputy Secretary of the Treasury. Until a new Deputy Secretary is named to fill the current vacancy, Zarate will report to David Aufhauser, Treasury General Counsel, who serves as the Chairman of the NSC policy coordinating committee on terrorist financing.** Within the U.S. Treasury, the new Office will provide policy guidance for the Financial Crimes Enforcement Network (FinCEN) bureau as it works with the financial sector, the law enforcement community, and foreign financial intelligence units to foster cooperation against domestic and international financial crimes. Source: <http://www.treasury.gov/press/releases/js77.htm>

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

## **Transportation Sector**

- 8. *March 04, Associated Press* — Miami screens ship-to-airport baggage.** James and Shirley Kelley returned from a weeklong Caribbean cruise Sunday and found that the hassle of lugging their bags to the airport had been taken out of their hands – literally. When they walked off their cruise ship and got to the front of the line at the baggage area of the Port of Miami, an airline official gave them their boarding passes while a federal baggage screener checked their belongings for traces of explosives. Moments later, their luggage was sent to a truck that would be sealed and sent to their airline at Miami International Airport. The Transportation Security Administration program, demonstrated for the news media Sunday, is about halfway through a 90-day trial run. **By screening bags at the port and sending them directly to the airport,**

security officials said, they reduce the likelihood that luggage could be tampered with while shortening security lines at the airport.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A32673-2003Mar 3.html>

9. *March 03, ABC News* — **Air traffic control glitch dents Japan's high-tech credibility. A weekend glitch in Japan's air traffic control system, which disrupted 1,600 flights and affected 270,000 passengers, has dealt another blow to the credibility of the country's high-tech industry.** The failure, the largest computer outage in Japan's aviation history, also prompted local media on Sunday to question the country's security preparedness at a time when it is gripped with a North Korean nuclear arms threat. **A flight data processing system, which covers the largest of Japan's four air control zones and automatically transmits data including flight numbers, went down for four hours on Saturday local time,** transport ministry officials said. **Due to a reprogramming hiccup, the main system and its backup went down immediately after being switched on, grounding all domestic flights for half an hour and forcing air controllers to operate the system manually.**

Source: <http://www.abc.net.au/news/justin/nat/newsnat-3mar2003-13.htm>

10. *February 28, Transportation Security Administration* — **TSA to have new passenger risk assessment and prescreening system .** Under Secretary of Transportation for Security Adm. James M. Loy announced on Friday that the Transportation Security Administration (TSA) has selected Lockheed Martin to develop a passenger risk assessment and prescreening system, also known as the Computer Assisted Passenger Pre-Screening System II (CAPPS II). CAPPS II is an automated screening system authorized by Congress in the wake of the Sept. 11, 2001 terrorist attacks. **It is a narrowly focused threat assessment tool, based on continuously changing intelligence information and threat priorities. As a resource management tool, it will help TSA direct limited on-site screening resources where they are most needed.** CAPPS II is a passive system activated by a traveler's airline reservation request. When the system is implemented, airlines will begin asking passengers for a slightly expanded amount of reservation information: the passenger's full name plus address, phone number and date of birth. This is the only public source information that TSA will collect for CAPPS II.

Source: <http://www.dot.gov/affairs/tsa1503.htm>

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

## Postal and Shipping Sector

11. *March 02, Texas City Sun* — **Ship explosion still threatens port.** Texas City's greatest threat of a terrorist attack is the same event that leveled the town in 1947. **A ship explosion in the port is the most likely way terrorists would attack the city,** according to Texas City's homeland security advisor Jerry Purdon. Purdon, the city's first homeland security specialist, has begun a public campaign to educate residents about the kinds of attacks they need to be prepared to address as a mainland resident in post-Sept. 11 culture. **While bioterrorism, nuclear attacks and chemical warfare are all possibilities, he said local officials believe terrorists would probably use Texas City to affect the American economy.** Purdon said he suspects terrorists could most likely use conventional means to attack the port because the population isn't high enough to warrant an organized bioterrorism attack or dirty bomb. "A shrimp boat loaded with explosive chemicals running in front of a larger ship or a truck loaded

with chemicals barreling into the plants or a plane flying over the plants is what Texas City needs to be concerned about," he said. **In 1947, a chemical reaction caused 2,341 tons of fertilizer-grade ammonium nitrate on a French freighter in the Texas City port to explode, creating one of the largest and deadliest industrial disasters in history.** Since then, preparation against industrial disasters has been in the forefront of Texas City community. Industrial safety issues have been widely addressed, but funding for security measures is inadequate, Purdon said.

Source: <http://texascitysun.com/report.lasso?WCD=2089>

[[Return to top](#)]

## **Agriculture Sector**

12. *March 03, expatica.com* — **Deadly virus hits poultry sector. The bird flu, a deadly and highly contagious virus, has hit some thirteen poultry farms in Gelderland, Netherlands, the agricultural ministry confirmed on Monday.** To stop the disease spreading further, Dutch agriculture minister Cees Veerman has ordered all chickens in a one-kilometre radius of the affected farms to be gassed. The European Commission also announced on Monday that it was imposing a temporary ban on the export of poultry products from the Netherlands. It is expected the ban will remain in force until Thursday. **As the latest outbreak of bird flu was confirmed at the weekend, additional precautionary measures have been taken in Barneveld, Scherpenzeel, and Renswoude, the epicentre of the crisis. All poultry has to stay indoors, farms are not allowed visitors, and it is forbidden to transport eggs for consumption.**

Source: <http://www.expatica.com/index.asp?pad=2.18.>>

13. *March 03, Associated Press* — **Fort Collins researchers develop DNA-based vaccine for West Nile. Colorado researchers decoding the deadly West Nile virus have developed the first DNA-based vaccine for animals and are using it in California to protect condors.** Two California zoos are already using the vaccine to protect America's largest and rarest bird, the endangered California condor. In December, the Los Angeles Zoo injected its 32 California condors, and the San Diego Zoo and Wild Animal Park quickly followed suit for its 35 condors. Within weeks, all the 196 California condors left in the world will be treated with the new DNA vaccine for West Nile. **Biologists who work with other endangered birds from spotted owls to whooping cranes are now considering whether to use the DNA vaccine for them, as well.**

Source: [http://www.pe.com/ap\\_news/California/West\\_Nile\\_Vaccine\\_99114\\_C.shtml](http://www.pe.com/ap_news/California/West_Nile_Vaccine_99114_C.shtml)

14. *March 02, Associated Press* — **Farmers struggle to replace drought-reduced hay supplies. Recent rain and snow may have brought an end to the long-term drought in Virginia, but farmers are still suffering from its effects, as supplies of hay are running low because of a drought-reduced harvest last summer.** Prices for the reduced supply of hay have soared this year, as farmers who usually harvest their own have been forced to buy extra this year. **The large, round bales of hay used by farmers usually cost \$20-\$25 but this year are selling for \$35-\$60, said Jimbo Tucker, owner of Tucker Livestock, a livestock buying company in Radiant.** One bale feeds 20 to 30 cattle for one day.

Source: <http://www.wset.com/showstory.hrb?f=na>>

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

## **Food Sector**

Nothing to report.

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

## **Water Sector**

Nothing to report.

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

## **Public Health Sector**

15. *March 03, Billings Gazette* — **State studies new tick-borne disease. Scientists believe an undiscovered Lyme disease-like illness is being transmitted by wood ticks in Montana, particularly in the Yellowstone River area from Livingston downstream to Forsyth.** The bulls-eye rash, fever, body aches, and lingering exhaustion caused by the illness have stumped doctors for at least a decade, said State Epidemiologist Todd Damrow in Helena. **Local, state, and federal scientists are launching an effort to crack the mystery. "We could have a new disease here, we just don't know right now," Damrow said.** "We don't know how prevalent it is, how pervasive or even the nature of the illness. Those are questions we need to address." The state receives a "handful" of reports each year of unexplainable illnesses believed to be caused by tick bites, Damrow said. The cases have been clustered in the Yellowstone River drainage, but reports have come in from both Helena and Missoula. In each instance, Lyme disease has been ruled out, as has Rocky Mountain spotted fever.

Source: [http://www.helenair.com/articles/2003/03/03/breaking/a010303\\_03\\_01.txt](http://www.helenair.com/articles/2003/03/03/breaking/a010303_03_01.txt)

16. *March 02, Boston Globe* — **Resistant-bacteria reports cause alarm. Five men in Boston, MA have been infected with a powerful, drug-resistant bacteria, strikingly similar to larger outbreaks in Los Angeles and San Francisco, CA.** Beginning last fall, doctors at the Fenway Community Health Center started seeing patients with pneumonia, sinus infections, and skin conditions caused by methicillin resistant staphylococcus aureus (MRSA), a germ normally caught only in hospitals by patients already seriously ill from other diseases. **Its appearance in the general community has alarmed health authorities. All five of the men have been treated and recovered without lasting complications, but doctors are worried about the broader emergence of bacteria so wily that they can outrun the best drugs that medicine can produce.** On the West Coast, outbreaks of similar staph infections have stricken hundreds of patients, with 928 reported in Los Angeles County jails during 2002. And earlier this year, public health agencies in LA and San Francisco both reported clusters of antibiotic-resistant bacterial infections in those cities' gay communities.

Source: [http://www.boston.com/dailyglobe2/061/metro/Resistant\\_bacteria\\_reports\\_cause\\_alarm+.shtml](http://www.boston.com/dailyglobe2/061/metro/Resistant_bacteria_reports_cause_alarm+.shtml)

17.

*March 02, Associated Press* — **Patient has smallpox–related infection. Doctors in California are trying to determine how an adult's eye became infected with the same virus used in the military's smallpox vaccination program.** The patient, who has not been identified, had been in close contact with someone who had been inoculated, health officials said. However, Dr. Jonathan Fielding, Los Angeles County's director of public health, said it remained unclear exactly how the patient became infected. The vaccine is made with a live virus that can be spread by touching a vaccination site before it has healed or by touching bandages, clothing or other material contaminated with the live virus. **"We really don't know how it happened – it could have happened in a variety of ways,"** Fielding said. **"What's important is they had direct contact with the person, rather than this being something that was just in the air."**

Source: <http://www.firstcoastnews.com/news/news–article.aspx?storyid=1148>

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

## **Government Sector**

**18. *March 03, Government Executive* — Interim field managers named at new border agencies.**

Homeland Security officials on Friday named 56 senior managers to direct regional operations at two new agencies designed to secure U.S. borders. **The managers, who will serve on an interim basis, will oversee regional inspection and investigation activities at the Bureau of Customs and Border Protection (BCBP), which will conduct inspections at 307 U.S. ports of entry, and the Bureau of Immigration and Customs Enforcement (BICE), an agency that will handle criminal investigations of U.S. customs and immigration laws.** Both bureaus were created on March 1, when their component agencies—the Customs Service, the Immigration and Naturalization Service (including the Border Patrol), the Federal Protective Service, and the Plant Protection and Quarantine unit of the Agriculture Department—moved into the Homeland Security Department.

Source: <http://www.govexec.com/dailyfed/0303/030303p1.htm>

**19. *March 03, NewsOK.com* — Terrorism a concern for schools.** Oklahoma education officials are creating attack–related safety policies in light of intelligence reports indicating terrorists may target schools. **Gayle Jones, safe and drug–free schools coordinator for the state Education Department, said terrorism in schools is virtually uncharted territory. "We've been dealing with substance abuse and violence,"** Jones said. **"This is a different topic we are having to tackle now. "We're right on target and trying to get accurate information and nonthreatening information out to the schools, as soon as we find a thorough way to do that."** In a nationwide survey of more than 650 campus police officers, 95 percent said their schools are vulnerable to a terrorist attack. Seventy– nine percent said their districts are not adequately prepared to respond to an attack.

Source: [http://www.newsok.com/cgi–bin/show\\_article?ID=993845e](http://www.newsok.com/cgi–bin/show_article?ID=993845e)

**20. *March 01, New York Times* — U.S. lists three Chechen groups as 'terrorist' and freezes assets. The United States designated three rebel groups in Chechnya on Friday as "terrorist organizations" linked to Al Qaeda and imposed a freeze on their American assets.** The groups were described as having been involved in the seizure of a Moscow theater last October in which 129 people died. **Richard A. Boucher, the State Department**

spokesman, said the groups on the list also had ties to the Taliban leaders ousted in Afghanistan. Russia has for many months asserted such a link existed as it has sought a global endorsement of its campaign against Chechen rebels. **The State Department identified the groups as Riyadus–Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs, the Special Purpose Islamic Regiment and the Islamic International Brigade.**

Source: <http://www.nytimes.com/2003/03/01/international/europe/01TER R.html>

21. *March 01, Associated Press* — **Homeland Security Dept. fully operational.** In the largest government reorganization since 1947, the Homeland Security Department became fully operational Saturday when 170,000 employees shifted from other areas of the federal bureaucracy to provide what Bush called "a united defense of our homeland." For now, the change is mostly on paper. Most of the department's workers, spread across the nation, will continue to show up for work at the same office, ship or airport as before. **Only about 10% – or 17,000 – work in the Washington area, and about 1,000 of them will work from the department's headquarters. The agency, with a \$33 billion first–year budget, is located at least temporarily at a secure office complex run by the Navy. It will take months or years for the department to become fully integrated with a permanent home and an identity all its own.**

Source: [http://www.usatoday.com/news/washington/2003-03-01-homeland-operational\\_x.htm](http://www.usatoday.com/news/washington/2003-03-01-homeland-operational_x.htm)

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

## Emergency Services Sector

22. *March 03, Washington Times* — **Bomb squad school.** In case of a war with Iraq and subsequent likely terrorist reprisals in the U.S., the battering down of hatches has fallen to several agencies, including the **Response to Terrorist Bombing school in Socorro, directed by principal investigator Van Romero.** "What's happening in Israel is what we're looking at here," he said. "The suicide bomber is a very real threat. It is something we are **planning for in the near future.**" There is a yearlong waiting list for these weeklong classes in New Mexico's sagebrush country. Training sessions for the country's only large explosives–training program have increased fourfold since the September 11 attacks for droves of "first responders" – people who show up first at accident or crime scenes. Overseen by the New Mexico Institute of Mining and Technology in Socorro, better known as New Mexico Tech, it employs 50 staff members teaching two classes a week of 35 to 40 students each. **The demand is such that classes are slated for 50 weeks a year, even during holidays. Its Justice Department funding has skyrocketed from \$3 million when the program began in 1998 to \$30 million for 2003.**

Source: <http://www.washingtontimes.com/national/20030303-80855260.htm>

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

## Information and Telecommunications Sector

23.

*March 03, Department of Homeland Security, National Infrastructure Protection Center* — NIPC Advisory 03-004: "Remote Sendmail Header Processing Vulnerability". The Remote Sendmail Header Processing Vulnerability allows local and remote users to gain almost complete control of a vulnerable Sendmail server. Attackers gain the ability to execute privileged commands using super-user (root) access/control. **This vulnerability can be exploited through a simple e-mail message containing malicious code.** Sendmail is the most commonly used Mail Transfer Agent and processes an estimated 50 to 75 percent of all Internet e-mail traffic. System administrators should be aware that many Sendmail servers are not typically shielded by perimeter defense applications. **A successful attacker could install malicious code, run destructive programs and modify or delete files. Additionally, attackers may gain access to other systems thru a compromised Sendmail server,** depending on local configurations. Sendmail versions 5.2 up to 8.12.8 are known to be vulnerable at this time. Due to the seriousness of this vulnerability, **the NIPC is strongly recommending that system administrators who employ Sendmail take this opportunity to review the security of their Sendmail software and to either upgrade to Sendmail 8.12.8 or apply the appropriate patch for older versions as soon as possible. Patches for the vulnerability are available from Sendmail at <http://www.sendmail.org>.** Additional information is available from CERT/CC at <http://www.kb.cert.org/vuls/id/398025>. Source: <http://www.nipc.gov/warnings/advisories/2003/03-004.htm>

24. *March 03, Department of Homeland Security, National Infrastructure Protection Center* — NIPC Advisory 03-003: "Snort buffer overflow Vulnerability". There is a buffer overflow in the Snort Remote Procedure Call normalization routines which can cause Snort to execute arbitrary code embedded within sniffed network packets. Depending upon the particular implementation of Snort **this may give local and remote users almost complete control of a vulnerable machine. The vulnerability is enabled by default.** Snort is a widely used Intrusion Detection System from Sourcefire. The affected Snort versions include all version of Snort from version 1.8 through current. **Snort 1.9.1 has been released to resolve this issue. More information can be found on the Sourcefire website: <http://www.sourcefire.com/services/advisories/sa022503.html>.** Source: <http://www.nipc.gov/warnings/advisories/2003/03-003.htm>

### Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 2 out of 4 <a href="https://gtoc.iss.net">https://gtoc.iss.net</a>	 Security Focus ThreatCon: 2 out of 4 <a href="http://analyzer.securityfocus.com/">http://analyzer.securityfocus.com/</a>
Current Virus and Port Attacks	
<b>Virus:</b>	#1 Virus in the United States: <b>WORM_KLEZ.H</b> Source: <a href="http://wtc.trendmicro.com/wtc/wmap.html">http://wtc.trendmicro.com/wtc/wmap.html</a> , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]

<b>Top 10 Target Ports</b>	137 (netbios-ns), 1434 (ms-sql-m), 80 (www), 113 (ident), 445 (microsoft-ds), 4662 (eDonkey2000), 135 (epmap), 6346 (gnutella-svc), 139 (netbios-ssn), 25 (smtp) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	---

[[Return to top](#)]

## General Sector

25. *March 03, USA Today* — **Terror arrest triggers 'mad scramble'**. U.S. officials said Sunday that the capture of al Qaeda military chief Khalid Shaikh Mohammed and the documents found in his midst have set off a frenzied manhunt to track other suspected terrorists in the United States and abroad. **With Mohammed's arrest Saturday in Pakistan came papers and communications equipment that already are helping in the hunt for other al Qaeda associates, a senior U.S. intelligence officer involved in the probe overseas said. Believing they had only 24 to 48 hours to act, CIA officials and FBI agents Sunday e-mailed names and information of suspected al Qaeda operatives, found on documents and computer files in the house where Mohammed was arrested, to their offices overseas. They're hoping operatives will recognize names and use the information to disrupt al-Qaeda cells and arrest suspects.** In particular, officials hope to arrest al Qaeda members in Kuwait and Qatar, where the U.S. military has bases. There's a "mad scramble going on" to track suspects, the senior intelligence officer said. "We have lots of names and lots of information."

Source: [http://www.usatoday.com/news/world/2003-03-02-topstrip\\_x.htm](http://www.usatoday.com/news/world/2003-03-02-topstrip_x.htm)

26. *March 03, Associated Press* — **Emergency services to simulate catastrophe in London.** Emergency services in London will soon simulate a "catastrophic incident" to test their ability to deal with terrorist attacks, the government said Monday. **In a written statement to lawmakers, Home Secretary David Blunkett said the exercise would cover mass evacuations and decontaminations. He said other exercises would cover possible disruption to the national gas supply and flood defenses. "Future planned exercises will cover a catastrophic incident in central London," Blunkett said. "It will be possible to test whether all key stakeholders are appropriately engaged and working together."** Blunkett gave no other details of the exercise, saying only it would "take place shortly."

Source: [http://story.news.yahoo.com/news?tmpl=story&p\\_w\\_o\\_e\\_n\\_g\\_e/eu\\_gen\\_britain\\_emergency\\_drill\\_2](http://story.news.yahoo.com/news?tmpl=story&p_w_o_e_n_g_e/eu_gen_britain_emergency_drill_2)

27. *February 28, Government Executive* — **New group to address 'disconnect' in security market.** A "tremendous disconnect" exists between federal, state and local government agencies and small- and medium-sized businesses looking to enter the counterterrorism market, the founders of a new homeland security organization said on Friday. **"We sort of sit between the government, industry and the small-business community so we can become a repository of information and ... disseminate that information back out,"** Preston McGee, a board member of the not-for-profit Homeland Security Leadership Alliance (HSLA), said during an introductory meeting. So far, the four-week-old organization has more than 70 members from 17 states and five countries, according to Sean Spence, the alliance's executive director. The diverse membership includes homeland security officials from all levels of government, executives from multibillion-dollar corporations and "little companies that

hardly even have revenues yet," Spence said.

Source: <http://www.govexec.com/dailyfed/0203/022803td1.htm>

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

## **NIPC Products & Contact Information**

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following NIPC products:

[NIPC 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](mailto: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](mailto: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](mailto: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.