



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 31 March 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The New York Times reports the Federal Emergency Management Agency suggests emergency planning around the Indian Point nuclear power plant should consider the threat of simultaneous terrorist attacks on the reactors as well as local bridges and roads used for evacuation. (See item [1](#))
- MSNBC reports identity theft costs banks \$1 billion a year -- involving home loans, new credit cards, fraudulent car loans -- and highlights the difficulty in positively identifying new customers. (See item [7](#))
- The New York Times reports federal authorities will order major security improvements at several of the nation's largest airports, after inspections showed that passenger planes taking off or landing at those airports would be vulnerable to attack by terrorists using shoulder-fired missiles. (See item [8](#))
- CNN reports the Centers for Disease Control and Prevention on Saturday extended its travel advisory for Severe Acute Respiratory Syndrome to include all of mainland China as well as Hanoi, Vietnam and Singapore. (See item [16](#))
- The CERT/CC has issued "Advisory CA-2003-12: Buffer Overflow in Sendmail." (See item [25](#))

DHS/IAIP 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](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: **Physical: High, Cyber: High**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

- 1. *March 28, New York Times* — Simultaneous attacks an issue for Indian Point. Emergency planning around the Indian Point nuclear power plant should consider the threat of simultaneous terrorist attacks on the reactors and on the area around them, the Federal Emergency Management Agency (FEMA) said today.** In a report requested by Representative Sue Kelly, a Republican whose district includes the plant, the agency said that planners should consider "other terrorist attacks occurring simultaneously" with an attack on the nuclear plant. Since the terrorist attack on the World Trade Center, the power plant, about 35 miles from Midtown Manhattan, in Buchanan, NY, has been seen as a potential target. **Some residents have voiced fears that if terrorists attacked Indian Point, they may also attack the bridges and roads that would normally serve as escape routes.** Kelly, who has called for a shutdown of the plant until questions about evacuation plans can be put to rest, had asked FEMA to address the impact of terrorism on emergency planning, among other issues. Her request came after Richard A. Meserve, the chairman of the Nuclear Regulatory Commission, criticized a state-commissioned report on emergency plans for Indian Point. Meserve said last month that the report "appears to give undue weight to the impact of potential acts of terrorism." **A lack of faith in the evacuation plans has prompted hundreds of officials to call for a shutdown of the plant. The four counties closest to Indian Point and the state emergency office have refused to certify the plans as up-to-date.** They have cited the state-commissioned report, by James Lee Witt, a former FEMA director, which concluded that emergency planning for the communities around the plant was inadequate.
Source: <http://www.nytimes.com/2003/03/28/nyregion/28INDI.html?ntem=ail1>
- 2. *March 27, Reuters* — TVA checking possible Sequoyah nuke lid leak. The Tennessee Valley Authority (TVA) Nuclear said Thursday it was checking a possible leak in the reactor lid at a Tennessee plant that may be similar to leaks at other reactors already expected to cost the U.S. nuclear industry over \$1 billion to repair. Indications of a leak were found in the reactor lid capping the 1,148 megawatt Sequoyah nuclear unit 1 in Soddy-Daisy along the Tennessee River in southeastern Tennessee, TVA spokesman Terry Johnson said. "Plant personal were doing an inspection on the reactor vessel head and they found indications of a boric acid leak on top of the reactor vessel," Johnson said. **The U.S. nuclear power industry was taken by surprise early last year when a hole eaten by boric acid from a cooling system was found in the lid of the FirstEnergy's 925 MW Davis-Besse plant in Oak Harbor, OH.** The discovery of the hole prompted the federal Nuclear Regulatory Commission to order special reactor vessel head inspections at all 69 of the nation's pressurized water reactors, which are the same design as Davis-Besse. The pressurized water reactors make up about 12 percent of U.S. power generation capacity. Companies that are willing to talk about the cost have estimated the reactor vessel head replacement at about \$60 million per unit. **The Sequoyah plant is a newer design than Davis-Besse, and had been deemed by the NRC to be of a lower susceptibility to vessel head corrosion.** TVA had said late last year that it did not expect to replace the reactor vessel heads at the two Sequoyah nuclear units. However, TVA's Johnson said Thursday those plans could change in light of the recent indications of a lid leak.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3738376**

3.

March 27, Reuters — **Nuclear Regulatory Commission sends inspection team to Michigan power plant.** The Nuclear Regulatory Commission (NRC) said it has sent inspectors to look into two recent electrical problems at the Palisades nuclear power plant located in Covert, Michigan. **The 789-megawatt plant, owned by CMS Energy Corp's Consumers Energy subsidiary, lost on Tuesday its connection to offsite electrical power sources. The plant's two emergency diesel generators started automatically to supply electricity to important plant safety systems.** The plant's diesel generators continue to supply power while the utility investigates the cause of the loss of offsite power and makes necessary repairs, the NRC said in a statement late on Wednesday. "Both diesel generators are operating, although one is sufficient to supply power to the reactor shutdown cooling system and other safety equipment," the agency said. The plant has been shut down since March 16 for refueling. **The NRC inspectors will also look into an March 18 incident when a circuit breaker at the plant failed and caused a fire that was confined to the circuit breaker. There were no injuries caused by the fire** The NRC said its report on the problems at the plant will be posted on the agency's Web site about 30 days after the inspectors finish their work.

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3738367

4. *March 26, The News & Observer (Raleigh, NC)* — **Nuclear Regulatory Commission finds risks at North Carolina plant.** The Nuclear Regulatory Commission (NRC) said overall that the Harris Nuclear Plant operated safely in 2002 but cited two problems of moderate risk related to the plant's safety systems. **The annual assessment of the plant owned by Progress Energy noted that a fire barrier between an auxiliary control panel room and a cable room was inadequate, and that rubber debris in a coolant line could impede flow. Both problems were described as moderate risks.** A Progress Energy executive said the plant had corrected the problems and was now in full compliance. The NRC regulates 103 commercial nuclear power plants by mandating requirements for design, construction and operation. **The oversight program includes seven general categories or "cornerstones" for safety. Of the 32 nuclear plants in the southeastern region, Harris was the only one requiring a higher level of inspections from the NRC during 2002.**

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3738046

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

5. *March 30, Washington Times* — **Bombs keep town on Oklahoma map. When the U.S. armed forces launched an invasion of Iraq to topple Saddam Hussein from power, the McAlester Army Ammunition Plant (MCAAP) suddenly burst into prominence on the public scene.** Producing the nation's bombs, MCAAP manufactures and delivers some 95 percent of the conventional bombs used by the United States. Whether it is Desert Storm or the wars in Yugoslavia, Afghanistan, or the current conflict in Iraq, the supply lines of the U.S.

military begin right here. **Yet the average McAlester resident not only has never been inside the vast 45,000–acre complex, but knows little about its importance. One reason can be traced to a persistent and somewhat widespread belief that too much attention on the complex could spawn deadly reprisals from terrorists.**

Source: <http://www.washingtontimes.com/national/20030330–83927232.htm>

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

Banking and Finance Sector

6. *March 28, Office of the Comptroller of the Currency* — **Telecommunications service priority (TSP) program: FBIIC policy on sponsorship of TSP for private sector entities.** The Financial and Banking Information Infrastructure Committee (FBIIC) has outlined its policy for the sponsorship of critical private sector entities' access to the Telecommunication Service Priority (TSP) Program administered by the National Communications System (NCS). **The NCS's TSP program assigns qualifying institutions priority treatment for the restoration or provisioning of telecommunication services in emergencies. Private–sector use of TSP must be sponsored by an authorized federal agency. The agency must first determine that the private–sector entity is considered critical to the performance of national security or emergency preparedness (NS/EP) functions.** For financial institutions, an NS/EP finding can be supported if the functions performed by the institutions are considered necessary to maintain the national economic posture during any national or regional emergency.

http://www.fbiic.gov/policies/TSP_policy.htm

Source: <http://www.occ.treas.gov/ftp/bulletin/2003–13.txt>

7. *March 27, MSNBC* — **ID theft costs banks \$1 billion a year.** Nearly 10,000 victims had home loans – totaling about \$300 million – taken out in their name in 2002 and another 68,000 had new credit cards issued in their name, said Christine Pratt, the author of the report and a senior analyst in TowerGroup's consumer credit practice. **She extrapolated the data from an annual Federal Trade Commission report issued in January. She then computed average losses per crime to arrive at her \$1 billion estimate. "And that number is probably conservative," she said. While the FTC received 161,000 identity theft complaints last year, the FBI estimates the actual number of victims is probably closer to 500,000 she said.** According to the FTC's 2001 report, the most recent for which data on auto loans is available, fraudulent car loans were one–fourth of all identity–theft based loans. **But the report's most disturbing assertion might not be the dollar figures. Pratt said that currently, banks have no way to positively identify new customers.** If their paperwork seems complete, they get the new account. The problem is exacerbated by intense competition in home mortgage refinancing, said Anthony Hsieh, CEO of Home Loan Center, an online lending firm. **Television advertisements encourage consumers to seek out "hassle–free" loan applications for which careful identity verification is anathema.**

Source: <http://www.msnbc.com/news/891186.asp?cp1=1>

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

Transportation Sector

8. *March 30, New York Times* — **Missile threat means new rules at airports.** Federal authorities will order major security improvements at several of the nation's largest airports **after inspections showed that passenger planes taking off or landing at those airports would be vulnerable to attack by terrorists using shoulder-fired missiles**, senior Bush administration officials said. The inspections, which began several weeks ago, are being conducted by a federal task force created by the White House late last year after terrorists linked to al Qaeda tried to shoot down an Israeli passenger plane on takeoff from an airport in Kenya in November. The two small, shoulder-fired missiles barely missed the plane. **Administration officials would not identify the airports that would be required to make major safety improvements, citing security reasons. But they said the list included several of the nation's busiest, and that the improvements would include new, round-the-clock security patrols and tightened electronic surveillance of the flight paths used for takeoffs and landings.** This week, dozens of National Guard troops were deployed to the Los Angeles International Airport to patrol the perimeter and road checkpoints, in part because of what security officials acknowledged was concern about shoulder-fired missiles. A spokesman for the Port Authority of New York and New Jersey, which manages Kennedy, La Guardia and Newark Liberty International airports, said it was aware of the missile threat and was responding to it. **American intelligence and law enforcement agencies say that al Qaeda and affiliated terrorist groups are believed to have an arsenal overseas of dozens of shoulder-fired missiles, including the American-made Stinger and the Russian SA-7**, and that others can be bought by terrorists on the black market for several thousand dollars each. Source: <http://www.nytimes.com/2003/03/30/national/30AIRP.html>

9. *March 28, CNN* — **Some airport screeners may be cut.** Some airports will have fewer passenger screeners this spring now that the government agency that hired them last year begins shrinking its work force. **As many as 3,000 screeners, or about one in 18, could lose their jobs.** The head of the Transportation Security Administration (TSA), James Loy, told a House Appropriations subcommittee that he wants to reduce the number of screeners from 54,000 to 51,000, and that layoff notices could begin going out April 1. By October 2004, the government plans to have 48,000 screeners with reductions through attrition and other steps, an agency spokesman said later. Last year, lawmakers capped the TSA's full-time screener positions at 45,000. Despite the cap, the agency hired 9,000 temporary employees, most on five-year contracts. **Rep. Harold Rogers, the Kentucky Republican who chairs the homeland security panel, said they hired too many.** The effort to trim the screening work force comes as Congress scrutinizes Loy's agency, now in its second year of existence. Lawmakers say they want to make sure the agency is doing what Congress intended, including tightening security for the transportation system. **Rogers said he is disappointed by what he said was the agency's emphasis on aviation security at the expense of highways, railroads, pipelines and ports. "You need to take a good hard look at our border and transportation systems," Rogers told Loy. "If we have a weakness, it will be found."** Source: <http://www.cnn.com/2003/TRAVEL/03/28/airport.screeners.ap/index.html>

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

Postal and Shipping Sector

10. *March 28, Reuters* — **War sees surge in sea freight rates. Thailand exporters and importers are not only facing a shortage of containers but have found their volume of goods fall by 20 per cent since last week's outbreak of war.** Mana Patram, director-general of the Port Authority of Thailand, said yesterday that cargo vessels cannot call on countries in the war zone such as Iraq and Kuwait. "They have to change course," he said. Most of the shipping routes to the Middle East and Europe are also one way, causing containers to pile up at the ports in those areas. "We now have to bring in empty containers from Hong Kong and Singapore. This has increased costs for exporters and importers," Mana said. **Higher oil prices have forced shipping firms to raise their rates by \$80 to \$100 per 20-foot container. And beginning on Tuesday, they will add a war risk surcharge of \$50 on each 20-foot container.**

Source: <http://www.nationmultimedia.com/page.news.php3?clid=6A05>

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

Agriculture Sector

11. *March 28, Expatica.com* — **Culling of chickens in buffer zone. Amsterdam Agriculture Ministry officials began culling an estimated 1.4 million chickens in a newly created buffer zone between the Rhine and Maas rivers on Friday to halt the spread of the avian flu to North Brabant province.** About 30 farmers in an area bordered by Opheusden, Druten and Beneden-Leeuwen were informed by telephone on Thursday that their poultry is being exterminated to create a "poultry-free zone". The zone is south of the Gelderse Vallei where the virus has been active since the start of March. Some 5 million chickens on farms have been culled on about 150 farms in this region.

Source: <http://www.expatica.com/index.asp?pad=2,18.>>

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

Food Sector

12. *March 27, Reuters* — **USDA picks system to test meat for bacteria. Federal meat inspectors have adopted a diagnostic system to detect disease-causing salmonella bacteria in meat, poultry, and egg products, the U.S. Agriculture Department (USDA) said on Thursday.** USDA said the system reduced the reporting time for testing meat products for salmonella by at least three days when compared to the current method. "This will be another tool that we will use to wage war on pathogens," USDA Undersecretary Elsa Murano said. USDA approved the system in April 2002 for detecting listeria monocytogenes in meat products. **The department said it would soon evaluate the system to detect E. coli O157:H7.**

Source: http://www.forbes.com/home_europe/newswire/2003/03/27/rtr922_279.html

13. *March 27, Agricultural Research Service* — **Radio frequencies blast bacteria in fruit juice. The Agricultural Research Service (ARS) has found that the radio frequency electric fields (RFEF) technique inactivates bacteria in apple juice without heating it. Although RFEF has been studied for more than 50 years as a pasteurization method, this is the first confirmed instance of a successful inactivation of bacteria using this technique in fruit**

juice. Conventional pasteurization using heat can affect the nutrient composition and flavor of fruit and vegetable juices. The RFEF technique itself is nonthermal because the inactivation is not produced by heat. However, when moderate heat is applied, the combined effect is much greater than the effect of either process used alone. RFEF could provide an alternative to pasteurization by heat. **According to David Geveke, a chemical engineer in the ARS, the RFEF process could be used to treat heat-sensitive products such as fruit juices, vegetable juices and liquid egg products.**

Source: <http://www.ars.usda.gov/is/pr/2003/030327.htm>

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

Water Sector

14. *March 28, Water Tech Online* — **EPA unveils funds to help water systems with security.** The U.S. Environmental Protection Agency (EPA) has announced a competitive assistance agreement program to support community drinking water utilities' efforts in **strengthening and enhancing the security of their infrastructure.** The program will focus on approximately 480 medium-sized community water systems that provide drinking water to more than 50,000 but less than 100,000 people, the agency said. **EPA said it allocated \$1.7 million for the program, which will complement its support to large drinking water systems serving 100,000 or more people and its grant program to states to help community water systems serving more than 3,300 but less than 50,000 people.**
Source: <http://www.watertechonline.com/news.asp?mode=4font>

15. *March 28, Atlanta Journal Constitution* — **Statewide water use restricted for good.** The Georgia Board of Natural Resources unanimously approved every-other-day schedules for homes and businesses to sprinkle lawns, wash vehicles, and fill swimming pools. **Most people will be able to use water outside three days a week; water-dependent businesses such as commercial car washes and nurseries are exempt.** The rules will be in effect statewide as soon as possible. Enforcement will be left to individual water providers, generally counties and cities, which can do anything from sending warnings to cutting off service. Many local governments choose to adopt their own regulations, but they must be in line with state rules. They also can enact tougher restrictions. **This is the first time Georgia has imposed outdoor watering restrictions when there's not a drought.**
Source: <http://www.accessatlanta.com/ajc/metro/0303/28drought.html>

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

Public Health Sector

16. *March 30, CNN* — **CDC extends SARS travel advisory.** The Centers for Disease Control and Prevention (CDC) on Saturday extended its travel advisory for Severe Acute Respiratory Syndrome (SARS) to include all of mainland China as well as Hanoi, Vietnam and Singapore. The CDC urged that anyone planning non-essential travel to mainland China and Hong Kong; Singapore; and Hanoi, Vietnam "may wish to postpone their trips until further notice." The CDC has been working closely with the World Health

Organization (WHO) to investigate the emergence of SARS, a deadly flu-like disease. Though a number of cases have been reported in Canada, the "CDC is not advising against travel to or from Canada because there is not evidence of widespread community transmission" there, the agency said in a statement. **Earlier, CDC officials said that 51 suspected cases of SARS have been identified in the United States. Worldwide, a total of 1,550 cases and 54 deaths have been reported from 13 countries as of Saturday, according to the WHO. Hong Kong is the world's most severely affected area, with 58 new cases of SARS reported on Friday alone, according to The Associated Press.** CDC officials are meeting planes, cargo ships and cruise ships coming either directly or indirectly to the United States from China, Singapore and Vietnam and distributing health alert cards to disembarking passengers. The CDC will distribute approximately 25,000 health alert notices daily to people returning from the affected regions at more than 20 ports of entry.

Source: <http://www.cnn.com/2003/HEALTH/03/29/sars.advisory/index.htm>

17. *March 28, Associated Press* — **Smallpox vaccine is reviewed. A second health care worker has died of a heart attack after receiving the smallpox vaccine, and officials are investigating whether vaccinations are to blame for cardiac problems seen in 17 people who have been inoculated.** The vaccine has never been associated with heart trouble, but as a precaution, the Centers for Disease Control and Prevention is advising people with a history of heart disease not to be vaccinated until further investigation is complete. CDC officials said yesterday there was some evidence the smallpox vaccine has played a role in heart inflammation. They were less certain whether three recent heart attacks were related to the vaccine.

Source: http://www.boston.com/dailyglobe2/087/nation/Smallpox_vaccine_is_reviewed_after_second_fatal_heart_attack+.shtml

18. *March 28, Associated Press* — **University of California to adopt Internet-based system to track medical errors.** A new Internet-based system that will track medical errors at five campus medical centers belonging to the University of California (UC) will follow the lead of other major health care providers that have enacted similar measures. **The system will allow hospitals to monitor trends in medication errors such as administering the wrong drug or the wrong dosage. It was also establish a "harm score system" for evaluating each error and comparing it with others.** Various health care providers have used the systems to improve quality and efficiency. In February, Kaiser Permanente, the state's largest HMO, rolled out a \$1.8 billion plan to give doctors and patients access to medical histories, test results, prescription information and other data, in part to reduce errors. **The University of California project is believed to be the first in the nation that links academic medical centers on a systemwide basis through the Internet.**

Source: <http://www.bayarea.com/mld/mercurynews/news/5504504.htm>

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

Government Sector

19. *March 28, Associated Press* — **FBI seeking to expand presence overseas.** The FBI plans to open offices in Kabul, Jakarta and eight other foreign capitals as part of a decade-long overseas expansion that officials say is crucial to meet the global threat of al Qaeda and other terrorist

groups. **The blueprint also calls for adding 30 new FBI personnel, including 17 agents, to the nearly 200 stationed at 46 locations around the world. Their importance was demonstrated during the afternoon of the Sept. 11 terror attacks, the FBI says, when agents in dozens of cities already were tracking down leads with the cooperation of local authorities in Germany, Canada, Great Britain and elsewhere.** Since the fall of 2001, about 500 agents and 200 support people have been working overseas on the terrorism investigation, along with the FBI agents known as permanent legal attaches, or "legats," who were already there. The agents are often directly involved with interrogation of terrorist suspects or criminals and sometimes submit questions to those doing the interviews, including CIA officers.

Source: http://www.washingtonpost.com/wp-dyn/articles/A42679-2003Mar_28.html

20. *March 28, Associated Press* — **U.S.: Iraqi terror-attack plans thwarted.** The State Department said on Friday it had information that Iraqi intelligence officers planned terrorist attacks against U.S. interests in two foreign countries. **In both cases, the operatives were arrested, terrorist material was confiscated and attacks were not carried out, spokesman Richard Boucher said. The United States has asked a number of countries to expel suspected Iraqi intelligence officers based on "the significant threat posed by their presence," Boucher said.** He declined to identify the two countries in the alleged terror plots. One of the countries is on the Arabian peninsula, said a U.S. counterterrorism official who spoke on condition of anonymity.

Source: http://www.washingtonpost.com/wp-dyn/articles/A43051-2003Mar_28.html

21. *March 28, Department of Homeland Security* — **New counternarcotics officer/U.S. interdiction coordinator.** Secretary of Homeland Security Tom Ridge and Director of the Office of National Drug Control Policy John Walters announced on Thursday **the designation of Roger Mackin to be Counternarcotics Officer and U.S. Interdiction Coordinator at the Department of Homeland Security.** Roger Mackin, a long-time veteran of the United States' international anti-drug efforts, will be the first individual to fill this new essential role at the Department of Homeland Security. **This new position will combine the duties of the United States Interdiction Coordinator, a currently held position within the ONDCP, with the new responsibilities defined with the Department of Homeland Security Counternarcotics Officer.** The position will consolidate several essential functions to fulfill the role of a federal anti-drug effort within the Department of Homeland Security, including coordinating the interdiction of illegal drugs entering the United States and tracking and severing connections between drug trafficking and terrorism.

Source: <http://www.dhs.gov/dhspublic/display?content=535>

22. *March 27, Associated Press* — **FBI Chief: Iraqi interviews helping U.S.** FBI interviews of thousands of Iraqis living in the United States have yielded valuable information about possible targets for U.S. troops in Iraq, FBI Director Robert Mueller said Thursday. **Some of the 6,700 Iraqis interviewed so far have described bunkers, tunnel systems, telecommunications networks, infrastructure, manufacturing plants and Iraqi military officials, Mueller and other U.S. law enforcement officials said. The intelligence, sometimes only fragmentary, is matched with information collected by the CIA and Defense Department and checked for accuracy before it is used to prosecute the war, the officials said.** They declined to provide specifics, which are classified, and expressed concern that too much detail could expose cooperating Iraqis or their family members in Iraq to retaliation. "What we have found in our

interviews around the country is a wealth of information," Mueller told the House Appropriations subcommittee that oversees the FBI and Justice Department budget. **The FBI is working toward a goal of interviewing about 11,000 Iraqis who have traveled to Iraq recently or have ties to Iraq's military. Many of these people are highly educated, have connections to Iraq's ruling classes and oppose the regime of President Saddam Hussein, officials said.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A38113-2003Mar 27.html>

23. *March 27, Washington Post* — **Taxpayers' online data protected, IRS says filing program had drawn fire.** The Internal Revenue Service's free online tax-filing program provides adequate protections for taxpayers and their confidential information, the agency said on Wednesday. **A group of consumer organizations charged this week that some companies participating in the program are using it to market products and services to taxpayers without properly obtaining the taxpayers' consent.** The initiative is "pro consumer," the IRS and Treasury Department said in a statement responding to the consumer groups. "It is a great deal for taxpayers to be able to file online for free," the statement said, noting that 2 million taxpayers have used the service so far. The program "also provides consumers with enhanced security and privacy protections," it said. **The agreement between the government and industry "requires industry members to protect taxpayer privacy and confidentiality," the statement added. "Unauthorized use of taxpayer information is a criminal offense."**
- Source: <http://www.washingtonpost.com/wp-dyn/articles/A34109-2003Mar 26.html>

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

Emergency Services Sector

24. *March 28, New York Times* — **911 calls by cellphone swamp California patrol.** Nearly all cellular 911 calls are answered by the highway patrol as a result of a law passed almost two decades ago, when cellphones were primarily in cars. **Now the calls are overwhelming the agency's call centers, resulting at times in long waits for callers and delays in getting calls to the appropriate agency, like local police or fire departments.** "Everyone's dispatch centers are being overloaded," said D. O. Helmick, commissioner of the California Highway Patrol. The problem of the number of calls is complicated by the difficulty of determining where each caller is, to determine how to forward the call – to the police department in Los Angeles or to the fire department in Orange County, for example. **California's situation is not unique, though it is extreme. Other states have different call centers set up and do not have as many cellphone users.** As of June 2002, according to the Cellular Telecommunications and Internet Association, California had 15.8 million cellphone subscribers – nearly half of the state's 34.5 million people. At that time the United States had about 128 million cellphone users nationwide.

Source: <http://www.nytimes.com/2003/03/28/national/28CALL.html>

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

Information and Telecommunications Sector

25. *March 29, CERT/CC* — **CERT Advisory CA–2003–12: Buffer Overflow in Sendmail.** **There is a remotely exploitable vulnerability in sendmail that could allow an attacker to gain control of a vulnerable sendmail server.** Address parsing code in sendmail does not adequately check the length of email addresses. An email message with a specially crafted address could trigger a stack overflow. **Successful exploitation of this vulnerability may cause a denial-of-service condition or allow an attacker to gain the privileges of the sendmail daemon, typically root.** Even vulnerable sendmail servers on the interior of a given network may be at risk since the vulnerability is triggered by the contents of a malicious email message. **Sendmail has produced patches for versions 8.9, 8.10, 8.11, and 8.12.** However, the vulnerability also exists in earlier versions of the code; therefore, **site administrators using an earlier version are encouraged to upgrade to 8.12.9.**
Source: <http://www.cert.org/advisories/CA-2003-12.html>
26. *March 27, Reuters* — **Al-Jazeera web site faces continued hacker attacks. Hacker attacks continued to plague the Web site of Arab satellite TV network al-Jazeera on Thursday,** as cyber-vandals replaced the news site with a stars-and-stripes logo saying "Let Freedom Ring." Both the Arabic site, at (<http://www.aljazeera.net>), and the English-language version at (<http://english.aljazeera.net>) could not be accessed on Thursday. Users who tried to log onto the site found a message that read, "Hacked by Patriot, Freedom Cyber Force Militia" beneath a logo containing the U.S. flag. "This broadcast was brought to you by: Freedom Cyber Force Militia," the site said. "God bless our troops!!!" **The al-Jazeera Web site has faced near-constant cyber attacks since an English-language version devoted exclusively to the war in Iraq was launched on Monday. The company also has had to search for a new home for the site after U.S.-based DataPipe said it could no longer host the site from the end of the month.** A spokesman from al-Jazeera said the company had moved its servers to a data center in France.
Source: <http://www.reuters.com/newsArticle.jhtml?type=internetNewsstoryID=2460457>
27. *March 27, The Associated Press* — **Anti-war protesters take digital turn. Anti-war demonstrators around the world are using a variety of technologies, including cell phones, e-mail, websites, text messages, and digital cameras, to plan, organize, rally support for, and execute protests against the conflict in Iraq.** These tactics are clear "proof that new technologies have revolutionized civil disobedience." (Summary thanks to Dartmouth ISTS.)
Source: <http://www.washingtonpost.com/wp-dyn/articles/A35652-2003Mar 27.html>
28. *March 27, Computerworld* — **Regional info-sharing network takes hold in Oregon. A public/private partnership in Oregon focused on homeland security information-sharing this month became one of the first grassroots efforts to move from concept to reality — and is already planning for an expansion to other states.** Oregon's Regional Alliance for Information and Network Security (RAINS), a partnership of more than 60 technology companies and government agencies, on March 14 officially launched a secure data-sharing network called RAINS-Net. The network is the first by-product of an effort to accelerate the adoption of cutting-edge homeland security information technologies. **Technologies from five Oregon-based IT companies form the backbone of the new 25-node network, which links local 911 centers, large banks and hospitals, Oregon's Department of Transportation, the city of Portland's Water Bureau, the Port of Portland and the Regional Maritime Coalition for the security of the Columbia River.** Fortix Inc. serves as the network's data

center and network host, and the Portland 911 center disseminates emergency information, including alerts. RAINS has already chartered a local chapter in Virginia and is in talks with several other unnamed states about expanding the network.

Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,79777,00.html>

Internet Alert Dashboard

| Current Alert Levels | |
|--|--|
|  <p>AlertCon: 1 out of 4 https://gtoc.iss.net</p> |  <p>Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/</p> |
| Current Virus and Port Attacks | |
| Virus: | #1 Virus in the United States: JS_NOCLOSE.E 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 | 80 (www), 137 (netbios-ns), 1434 (ms-sql-m), 25 (smtp), 445 (microsoft-ds), 139 (netbios-ssn), 4662 (eDonkey2000), 113 (ident), 0 (---), 53 (domain) Source: http://isc.incidents.org/top10.html ; Internet Storm Center |

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

General Sector

29. *March 30, New York Times* — Iraqis threatening new suicide strikes against U.S. forces.

One of Iraq's top leaders said today that Saddam Hussein's government was ready to meet the overwhelming military superiority of the United States **by resorting to widespread suicide attacks against Americans and British troops "and all who support them," both inside Iraq and elsewhere in the Arab world.** Vice President Taha Yassin Ramadan, ranked No. 3 in the Iraqi hierarchy, said at a news conference that the soldier who killed four Americans in a suicide attack Saturday outside the city of Najaf was the first in a wave of Iraqis and other Arab volunteers ready to become "martyrs." Arabs outside Iraq, he said, should help "turn every country in the world into a battlefield." **Although overheated polemics are a feature of the Baghdad leadership, no member of the group around Hussein has ever explicitly embraced suicide attacks as a potential Iraqi weapon.**

Source: <http://www.nytimes.com/2003/03/30/international/worldspecial/30BAGH.html>

30. *March 28, Reuters* — France: 4-color alert system adopted for threats. France announced

a revamp of its terror threat alert system to a four-color gauge on Thursday and said it was on "orange alert," under which terrorist acts are seen as plausible. The new system grades alerts as yellow, orange, red and – the highest level reserved for "major" risks – scarlet. Separately, the Environment Ministry said an April meeting of environment ministers

of the G8 group of industrialized nations had been moved to Paris from the western city of Angers, citing "the evolution of the international situation." A spokeswoman declined to comment on a newspaper report that security fears were behind the venue change.

Source: http://www.boston.com/dailyglobe2/087/nation/4_color_alert_system_adopted_for_threats+.shtml

31. *March 28, Associated Press* — **U.S. Arabs, Muslims reporting hate crimes.** Muslim, Arab and Sikh groups say reports of backlash crimes are trickling in, and they fear an increase if the war in Iraq drags on. Advocates who track such incidents say they've heard about a dozen potential hate crimes – most involving verbal harassment or property damage to Arabs, Muslims and Sikhs – since the war began last week. **"The longer the war goes on and the higher the number of American casualties there, I think probably you can make a correlation there would be more hate crimes and harassment against Arab-Americans and those perceived to be,"** said Laila Al-Qatami, a spokeswoman for the **American-Arab Anti-Discrimination Committee.** The Council on American-Islamic Relations has distributed "safety kits" to mosques, community leaders and others with tips on preventing hate crimes, developing relationships with law enforcement, safeguarding legal rights and responding to anti-Muslim incidents.

Source: http://www.washingtonpost.com/wp-dyn/articles/A42609-2003Mar_28.html

[[Return to top](#)]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate serves as a national critical infrastructure threat assessment, warning, and vulnerability entity. The IAIP 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 IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Warnings](#) – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. 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.

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

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

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

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

Contact DHS/IAIP

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

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.