



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 28 April 2004

Current Nationwide
Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)

www.whitehouse.gov/homeland

Daily Overview

- The General Accounting Office reports that since a successful terrorist attack on sites containing nuclear weapons could have devastating consequences, the Department of Energy needs an effective safeguards and security program. (See item [3](#))
- The Associated Press reports a Delta Air Lines flight headed from Los Angeles to New York was diverted to Salt Lake City after a man with a butane lighter alarmed the flight crew. (See item [14](#))
- eSecurity Planet reports that security researchers have discovered a serious boundary error vulnerability in multiple versions of Microsoft's Windows platform and warned that attackers could hijack systems via Windows Explorer and Internet Explorer. (See item [31](#))
- Security Focus has raise ThreatCon to Level 3, citing an increased need for vigilance. Please refer to the Internet Alert Dashboard.

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [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 Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP 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. *April 27, Reuters* — ChevronTexaco halts Wales refinery unit. U.S. oil major ChevronTexaco has stopped production from its 32,500-barrel-per-day alkylation unit at its 210,000 bpd Pembroke refinery in Wales, gasoline traders said on Tuesday, April

27. The unit produces alkylate, a key component in gasoline production. The halt in production was unscheduled and it was unclear what caused the problem, traders said. A ChevronTexaco spokesperson said that the company could not comment on refinery operations, but said that there had been no disruption to supply. The Pembroke refinery exports gasoline to the United States. **It is one of the few European refineries capable of making the tough new specification gasoline used in the states of New York and Connecticut.** To date in April, the refinery has exported two 33,000–37,000 tons of the new specification gasoline cargoes to the United States in the build up to the peak summer driving season.

Source: http://biz.yahoo.com/rc/040427/energy_gasoline_refinery_1.ht ml

- 2. *April 27, Associated Press* — Greenspan seeks to grow natural gas trade. The United States needs to expand the global trade in natural gas as a way to prevent future sharp price increases from harming its economy, Federal Reserve Chairman Alan Greenspan** said Tuesday, April 27. Greenspan said a dramatic rise in recent years in the price of both oil and gas for delivery six years into the future was almost certain to have an impact on the U.S. economy. However, he said the impact was likely to be greater for users of natural gas because they had no global supply to cushion price increases. Greenspan said the fact that worldwide imports account for 57 percent of global oil consumption but only 23 percent of natural gas consumption showed the growth potential for trade in natural gas.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A46308-2004Apr 27.html>

- 3. *April 27, General Accounting Office* — GAO-04-623: Nuclear Security: DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat (Report). A successful terrorist attack on Department of Energy (DOE) sites containing nuclear weapons or the material used in nuclear weapons could have devastating consequences for the site and its surrounding communities. Because of these risks, DOE needs an effective safeguards and security program.** A key component of an effective program is the design basis threat (DBT), a classified document that identifies the potential size and capabilities of terrorist forces. The terrorist attacks of September 11, 2001, rendered the then-current DBT obsolete. The General Accounting Office (GAO) examined DOE's response to the September 11, 2001, terrorist attacks, identified why DOE took almost two years to develop a new DBT, analyzed the higher threat in the new DBT, and identified the remaining issues that need to be resolved in order for DOE to meet the threat contained in the new DBT. **GAO is making a series of recommendations to the Secretary of Energy to strengthen DOE's ability to meet the requirements of the new DBT and to strengthen the department's ability to deal with future terrorist threats.** Highlights: <http://www.gao.gov/highlights/d04623high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-623>

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

Chemical Industry and Hazardous Materials Sector

- 4. *April 27, The Grand Rapids Press (MI)* — Agency marks 15 years of protecting against chemical emergencies.** Long before September 11 defined danger, a Kent County (MI) group was planning for mass disaster. **Tuesday, April 27, is the 15th anniversary of the Kent County Local Emergency Planning Committee, which is charged with saving lives in case of a release of hazardous materials.** As part of her work with the Kent County Sheriff's

Department, Sue Barthels has been involved with the emergency planning committee since its inception. She now is committee coordinator and says the world has finally caught up with the work they started in 1989. She says the tragedies of the past few years have shown the need for emergency preparedness and for agencies working together. Now the committee is more involved in updating plans so they meet federal standards. **In addition to tracking where chemicals are stored, the committee educates people on what to do in an emergency, what to put into a shelter kit and how to protect families.**

Source: http://www.mlive.com/news/grpress/index.ssf?/base/news-14/10_83077545248040.xml

5. *April 27, The Daily Nonpareil (Council Bluffs, IA)* — **Company offers \$50,000 reward to help solve chemical theft. Wickman Chemical is offering a \$50,000 reward for information leading to the return of nearly \$200,000 in agricultural chemicals stolen last week — the result of a bad check scam.** Erich Wickman, the company's owner, said nearly 7,000 pounds of herbicides were "sold" April 16 to a young man claiming to represent a group of Minnesota farmers. The company found out the next Monday the check was bogus. Wickman said the man, who appeared to be in his early 20s, provided what looked like legitimate paperwork, including a valid Minnesota permit number, to purchase the chemical and his banker's phone number. Wickman said the company checked the permit number and called the alleged banker, who approved the check. The Cass County Sheriff's Office said the investigation is continuing and is being taken very seriously. Wickman said the chemicals were not explosive and it is likely they will be sold or used as intended, and not for terrorist purposes. Officials say the suspected thief may be from South Dakota or Minnesota.

Source: http://www.zwire.com/site/news.cfm?newsid=11394309&BRD=2554&PAG=461&dept_id=507134&rfti=6

6. *April 27, General Accounting Office* — **GAO-04-361: Nonproliferation: Delays in Implementing the Chemical Weapons Convention Raise Concerns About Proliferation (Report).** Originally published on March 31. The Chemical Weapons Convention (CWC) bans chemical weapons and requires their destruction by 2007, with possible extensions to 2012. The General Accounting Office (GAO) was asked to review (1) member states' efforts to meet key convention requirements, (2) OPCW's efforts in conducting inspections to ensure compliance with the convention, and (3) Russia's efforts to destroy its chemical weapons stockpile. **The GAO found that the CWC has helped reduce the risks from chemical weapons, but CWC member states are experiencing delays in meeting key convention requirements as the CWC's goals have proven more difficult to achieve than anticipated.** The GAO believes the CWC has made important contributions to nonproliferation and further clarified this point in this report. The Departments of State and Defense expressed concern that GAO included a policy option to condition future U.S. aid on development of a credible Russian chemical weapons destruction plan. However, GAO provides several policy options, including increasing aid to Russia.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-361>

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

Defense Industrial Base Sector

7.

April 27, The Sun (WA) — **Naval station, submarine base to merge. In a cost-savings move, two major Navy home ports, located eight miles apart, will merge into one beginning in June, the Navy announced Monday, April 26. After the consolidation, Naval Station Bremerton and Naval Submarine Base Bangor, both located in Washington State, will be no more. Instead they will be called Naval Base Kitsap.** The consolidation, following a Navywide trend to merge commands and bases for efficiency purposes, will save the Navy between \$1 million and \$2 million per year by eliminating more than 30 military and civilian jobs, Navy sources said. The Navy is trying to save \$40 billion over four years in order to build more ships. Virtually every Navy program or service is being examined for cost-saving measures. The Naval Base Kitsap proposal went through the approval process for more than six months back at Navy headquarters in Washington, D.C. Secretary of the Navy Gordon England finally gave it the go-ahead late last week. **The merger of the two Kitsap bases follows the Navy's new business model of regionalizing services for sailors and families and eliminating those it deems repetitive.**

Source: <http://www.thesunlink.com/redesign/2004-04-27/local/459537.s.html>

8. *April 26, Federal Computer Week* — **DoD decentralizes Wi-Fi.** The Department of Defense's new wireless fidelity (Wi-Fi) policy seeks help from many of its agencies to ensure their employees and contractors use caution when operating wireless computer devices at military installations. **The chief information officer and DoD's Office of Networks and Information Integration (NI2) oversee and monitor the new Wi-Fi policy.** However, the undersecretary of Defense for Intelligence, the Chairman of the Joint Chiefs of Staff, the U.S. Strategic Command, the Defense Information Systems Agency and department staff officials all get roles in the new policy. **The policy mandates that military and industry officials do not use wireless devices to store, process and transmit classified information without approval from the various agencies and department officials.** It was issued April 14.

Source: <http://www.fcw.com/fcw/articles/2004/0426/web-wifi-04-26-04.asp>

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

Banking and Finance Sector

9. *April 28, The New Zealand Herald* — **Online scam sparks bank security scare. A sweeping review of internet banking security in New Zealand is being done after international criminals stole up to \$100,000 from online customers. Under new security measures being considered by banks throughout New Zealand, online customers may be given withdrawal restrictions, sent passwords through text messages and given security cards to allow them access to their bank accounts.** The move comes after banks were hit by an internet scam in which up to \$100,000 was stolen from several customers. The national manager of the police e-crime laboratory, Maarten Kleintjes, said the scam artists, operating from Estonia and Latvia, used fake identities and tricked customers into emailing their personal banking details. People in New Zealand were then employed to send money into overseas accounts. Those making the transactions thought they were working for a legitimate company. Kleintjes said countries such as New Zealand and Australia, which had less-secure banking systems than European nations such as Finland, were targets of the scams.

Source: <http://www.nzherald.co.nz/storydisplay.cfm?storyID=3563160&thesection=technology&thesubsection=general&thesecondsubsection=>

10. *April 27, Sydney Morning Herald (Australia)* — **Australian banks targeted in Windows hack attack.** Malicious attackers in Brazil, Germany and the Netherlands tried to use a vulnerability in Windows to break into some of Australia's largest financial institutions, including at least three banks, according to the Atlanta, GA–based security firm, Internet Security Systems (ISS). ISS (Australia) managing director Kim Duffy said the attacks were picked up by ISS's Global Threat Operations Center on Thursday, April 22. He said that **by Friday, April 23, the attacks had escalated significantly "and by lunch time we became aware that hackers were trying to infiltrate many of Australia's largest financial institutions."** **The vulnerability was one of 14 sealed by the patch issued along with Microsoft Security Bulletin MS04–011 on April 13.** "A successful attack over the weekend would enable hackers to have full remote control of important servers and have the potential, depending on the target server's configuration, to compromise an institution's most sensitive data. Whilst the attacks were primarily aimed at financial institutions, the reality is that they could, at any moment, switch to any entity operating with a vulnerable Microsoft SSL (Secure Socket Layer) server," Duffy said.
Source: <http://www.smh.com.au/articles/2004/04/27/1082831541968.html>

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

Transportation Sector

11. *April 27, Occupational Safety and Health Administration* — **OSHA, airline group renew alliance.** An Alliance between the Occupational Safety and Health Administration (OSHA) and a group of 13 airlines and the International Air Transport Section of the National Safety Council (NSC) was renewed recently to continue building on successes realized since the agreement was first launched in November 2002. **OSHA Administrator John Henshaw signed the two–year renewal on April 20 for the Airline Industry Alliance that provides participants with more opportunities to continue advancing workplace safety and health.** "Our thirteen member Airline Group recognized and appreciated the synergies which resulted from the first year of our Alliance with OSHA and the National Safety Council," said Barry Brown of Southwest Airlines, speaking on behalf of the Alliance participants.
Source: http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_tabl e=NEWS_RELEASES&p_id=10805
12. *April 27, Reuters* — **U.S. airline recovery still unsteady. Several factors, including high jet fuel prices, the security and hassle factor at airports and low aircraft use rates, are preventing a full–fledged U.S. airline recovery, say two leading aviation economists.** "Air travel is not going to come back to the old trend," said William Swan, chief economist at Boeing Commercial Airplanes, referring to a time when demand was strong, even for expensive airfares. "It's going to run parallel to the long–term trend." While load factors, measuring what percentage of seats are sold, are running fairly high presently, "as it turns out, it's an absolutely worthless indicator of what's going on," Swan said. Instead, he focuses on the rate of aircraft utilization. Since the September 11 attacks, those rates remain low except for the next generation of Boeing 737s. At an informal poll of several hundred aviation professionals conducted at the start of the Airfinance Journal conference in New York, more than three–quarters of the participants said they were neutral to fairly pessimistic about the state of

the U.S. airline industry.

Source: http://www.cnn.com/2004/TRAVEL/04/27/bt.us.airline.unsteady_reut/index.html

13. *April 27, Associated Press* — **Middle East airlines fly high.** At a time when the airline industry is witnessing the worst downturn in the modern history of aviation, airlines in the Gulf are expanding and carrying more passengers. "Places like Doha and Dubai have created themselves as hubs, with very good airports and tourism infrastructure," said Bikram Vohra, a consulting editor to The Middle East Aviation Journal. Vohra added that the increasing flow of expatriate workers moving to the Gulf also contributes to the growth of the region's airline industry. **Andy Critchlow, Gulf correspondent for the Middle East Economic Digest, points out that the airlines like Emirates and Qatar Airways enjoy advantages including a key geographical location in the middle of the world and relatively low fuel costs and taxes.** Global aviation has been hit hard by the September 11, 2001, terrorist attacks in the United States, the Iraq war, and most recently, the SARS epidemic in Asia. **But according to the Geneva-based International Air Transport Association, the Middle East recorded an 11.1 percent increase in passenger traffic, while world passenger traffic dropped by 4.2 percent in the period between January and October 2003.**

Source: <http://www.cnn.com/2004/TRAVEL/04/27/bt.mideast.airline.ap/index.html>

14. *April 27, Associated Press* — **Los Angeles flight to New York diverted to Utah. A Delta Air Lines flight headed from Los Angeles to New York was diverted to Salt Lake City on Tuesday, April 27, after a man with a butane lighter alarmed the flight crew, officials said.** Flight 1986 left Los Angeles International Airport about 8 a.m. PDT and landed about two hours later at Salt Lake City International Airport. The plane's 139 passengers were taken off the craft to be re-screened while the man who had been "acting strangely" was questioned by FBI and Transportation Security Administration agents, airport spokesperson Barbara Gann said. Dogs sniffed passenger bags and agents combed through the plane, which was expected to take off again for New York's Kennedy Airport early in the afternoon.

Source: <http://www.wjla.com/news/stories/0404/142697.html>

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

Postal and Shipping Sector

15. *April 27, Japan Times* — **Panel proposes Japan Post be privatized. A key policy-setting panel on Monday, April 26, finalized an interim report proposing that Japan Post be fully privatized in 2012 at the earliest and maintain its nationwide network of post offices.** But experts said the government must overcome many hurdles before it decides next fall on the final postal privatization plan, a key policy goal of Prime Minister Junichiro Koizumi. In the interim report, the panel calls for complete postal privatization after a transitional period of between five and 10 years beginning in 2007. Defining the main purpose of privatization as improving the level of public convenience, the panel proposes that nationwide mail services, postal savings, and postal insurance be maintained so that "all the people" could use the services. **The report proposes that Japan Post be allowed to take over or tie up with other companies to seek profitability in such business as mail and parcel delivery services.** The government-backed corporation is currently prohibited from entering new business fields.

Source: http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nb2004042_7a2.htm

16. *April 27, Associated Press* — **FedEx plane lands on highway.** A single-engine plane carrying FedEx cargo made an emergency landing on a highway early Tuesday, April 27, and a passing truck knocked off a wing but no one was hurt, officials said. **The single-engine turboprop Cessna was on a flight from Memphis, TN, to Monroe, LA,** said Sandra Munoz, a spokesperson for FedEx. It landed on a four-lane stretch of U.S. 61, where the truck hit it. The cargo will be sent by truck to Memphis and will be flown to Monroe, Munoz said. The plane experienced engine trouble about 35 miles south of Memphis, but the cause of the problem wasn't immediately known, Federal Aviation Administration spokesperson Christopher White said. It was operated by Baron Aviation under contract with FedEx, Munoz said. The plane is what the shipping giant refers to as a feeder plane, which is used to make short deliveries to areas that might not be serviced by a full-size jet.

Source: <http://www.wcnc.com/sharedcontent/nationworld/nationprint/042704ccjccwnatplane.16797fdc4.html>

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

Agriculture Sector

17. *April 27, Reuters* — **Thailand delays declaring itself free of bird flu. Thailand has delayed for a second time its plan to declare the country free of bird flu after a new outbreak of the virus was found, a government official said on Tuesday, April 27.** "We could not announce that the country is free of bird flu as a new fresh outbreak has been found at a chicken farm," said Yukol Limlamthonbg, head of Thailand's Livestock Development Department. "We will need to wait for another 21 days to ensure the virus is under control, then we can announce it," Yukol said. The outbreak was found in chickens at a farm in the northern province of Uttraradit on April 19, Yukol said. **The Agriculture Ministry had originally hoped to announce that the country was free of the virus on April 9.**

Source: <http://www.alertnet.org/thenews/newsdesk/BKK157837.htm>

18. *April 26, Reuters* — **Animal ID program. The U.S. Department of Agriculture (USDA) has \$18.8 million to launch a U.S. animal identification system this year, Undersecretary Bill Hawks said on Monday, April 26.** With nationwide animal ID, officials would be able to trace within 48 hours the herdsmates of suspect animals in cases of a disease outbreak. **It could cost \$550 million over five years to implement an animal ID system for food animals, according to U.S. Animal Identification Plan, a state-federal-industry consortium.** Costs are pegged at \$73 million for the first year, mainly to create a network for issuing "premises" ID numbers to farms, ranches, feedlots, packing plants, and other places where animals congregate. The Bush administration has requested \$33 million in fiscal 2005, which begins October 1, for animal ID work.

Source: http://www.agriculture.com/worldwide/IDS/2004-04-26T195119Z_01_N26373030_RTRIDST_0_FOOD-MADCOW-TRACEBACK-REPEAT.html

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

Food Sector

19. *April 27, USAgNet* — **Mexico to maintain ban on U.S. beef imports.** Mexico's Agriculture Ministry said on Monday, April 26, it would maintain a partial ban on U.S. beef imports introduced last year due to mad cow health fears. **Javier Trujillo, the ministry's animal and plant health chief, said that Mexican officials who visited U.S. plants in March were unhappy at methods used for deboning beef.** "The practical consequence of this is that none of the plants that are accredited by Mexico are going to be accepted when they use this method," Trujillo said. Mexico forbade U.S. beef imports in December after a case of mad cow disease was discovered in Washington state, but it eased the ban in March and allowed 40 percent of the previously outlawed beef to be imported. **Mexico will maintain its ban on imports of U.S. boned beef, pet food, and live cattle following the plant visits, Trujillo said.**
Source: <http://www.usagnet.com/story-national.cfm?Id=451&yr=2004>
20. *April 26, Reuters* — **EU paves way to end ban on new GM foods. The European Union (EU) was expected on Monday, April 26, to soon end a five year ban on approvals of new genetically modified (GM) foods, paving the way for a biotech maize product to hit Europe's supermarket shelves.** The opportunity to end the ban came after a meeting of the EU's 15 agriculture ministers failed to break a longstanding deadlock on whether to approve a maize variety known as Bt-11. The European Commission now has the legal power to rubberstamp a request for imports of Bt-11, although there is no formal time limit for the EU executive to act. The last EU approval of any GM product was in October 1998 for a type of carnation. The last food product, a type of maize, was approved in April that year.
Source: http://www.agriculture.com/worldwide/IDS/2004-04-26T164735Z_01_L263032_RTRIDST_0 FOOD-EU-GMO-UPDATE-2.html
21. *April 26, Food and Drug Administration* — **Safety of imported foods strengthened under proposed rules. The Food and Drug Administration (FDA) is issuing a proposed rule covering the use of private sampling services and laboratories in connection with imported food.** Once finalized, the rule will strengthen the safety and wholesomeness of the U.S. food supply by helping to assure the integrity and scientific validity of data and results submitted to FDA. **The new regulations would require samples to be properly identified, collected, and maintained; mandate that private laboratories use validated or recognized analytical methods; and direct private laboratories to submit the results directly to FDA.** The proposal also would require importers to provide notice to FDA about the use of a sampling service or a private laboratory to sample and test food that is subject to an FDA enforcement action. Imports of food are rapidly rising and last year reached more than six million shipments. FDA estimates that importers hire more than 100 private laboratories to generate analytical data in support of claims that imported food products comply with U.S. laws.
Source: <http://www.fda.gov/bbs/topics/news/2004/NEW01057.html>
22. *April 26, Associated Press* — **High lead levels in Mexican candy.** Tracking the source of the dangerously high levels of lead often found in Mexican candies sold in the U.S. requires going back to the source, the fields where the hot chilies that are the candies' key ingredients are grown. The Orange County Register reported Monday, April 26, that the chilies are clean when harvested in the states of Aguascalientes and Zacatecas, but often become tainted on the way to the factories where candies are manufactured. **The result, the Register reported, is that**

authorities who have performed more than 1,500 tests on Mexican candy in the U.S. since 1993 have found high levels in one out of every four samples. Lead poisoning can cause irreversible brain and nerve damage and result in lowered intelligence and behavioral problems, particularly in children. **State officials have estimated that as many as 15 percent of California children who suffer lead poisoning, or about 3,000 over the past three years, have eaten Mexican candy.**

Source: http://cbsnewyork.com/healthwatch/health_story_117175628.htm

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

Water Sector

23. April 27, Sacramento Bee — U.S. may cut water to states. The federal government is threatening to impose unilateral water cutbacks on California, Arizona, and Nevada if the three states can't come up with a plan to deal with a historic drought on the Colorado River. Following five years of dry weather, the two largest reservoirs on the Colorado are roughly half-empty and dropping fast, and Interior Department officials are urging water agencies to work together on a contingency plan or have one imposed on them. "We need the three basin states to get their act together and deal with shortages," said Assistant Interior Secretary Bennett Raley in a recent meeting with water officials from California, Arizona, and Nevada. If the three states can't work out a plan, he said, the Interior secretary "will have to do it." For years, Los Angeles, Las Vegas, and other fast-growing cities in the region have depended on surplus water from the Colorado, supplies that exceed their entitlements. **Now, the Southwest is shifting to a much drier period, and states are facing not only the loss of surplus but also cutbacks that could affect tens of millions of people.**

Source: http://www.sacbee.com/content/politics/story/9076337p-100022_38c.html

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

Public Health Sector

24. April 27, Channel News Asia — Beijing acts to prevent SARS outbreak from worsening. More than 600 people in Beijing have been isolated as the Chinese capital acts to prevent a Severe Acute Respiratory Syndrome (SARS) outbreak from worsening ahead of the busy Labor Day holidays. So far there are six suspected and two confirmed cases in Beijing and Anhui province. One confirmed SARS patient is said to be recovering and in a stable condition. **To investigate further, all laboratories in China have been placed under intense scrutiny.** The infections started with two lab workers at the Beijing's Center for Disease Control contracting the virus. One of them reportedly spread the virus to a nurse who in turn infected her family members in the eastern province of Anhui. **An anti-SARS headquarters has been set up in Beijing, and in hospitals, everyone with a high fever is closely monitored.**

Source: <http://www.channelnewsasia.com/stories/eastasia/view/82082/1/.html>

25. April 27, Associated Press — Fish Handler's Disease on rise in Maryland. Doctors believe rockfish in the Chesapeake Bay are carrying Mycobacterium marinum, a bacterium that

watermen call "fish handler's disease." Maryland state scientists estimate it has spread to 50 percent of rockfish in some areas of the bay. The Virginia Institute of Marine Science, however, estimates 76 percent of rockfish baywide are infected. "I think there is a clear, human health concern that hundreds of people will be out fishing for rockfish at the start of the season, and very few are aware there is a prevalent disease with these fish," said Howard R. Ernst, a Naval Academy professor. Mycobacterium is a threat, said Martin Gary, a Department of Natural Resources fisheries ecologist, but it "isn't showing up in any way, shape or form that shows we're losing fish." Gary says fish handler's disease suffers an exaggerated reputation because several infections that aren't mycobacteriosis get lumped together as fish handler's disease. Maryland doesn't keep records of how many people catch it, but surgeons at the Curtis National Hand Center in Baltimore say they see two to three new cases every month.

Source: <http://www.nola.com/newsflash/national/index.ssf?/base/national-1/1083067742161690.xml>

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

Government Sector

26. *April 27, Department of Homeland Security* — Partnering with the nation's universities.

Through the Homeland Security Centers of Excellence the Department of Homeland Security (DHS) is encouraging universities to become centers of multi-disciplinary research where these important areas of inquiry can be analyzed, debated and shared. **For example, the academic community will play a critical role in securing America. To facilitate this involvement, DHS has established university-based Homeland Security Centers of Excellence (HS-Centers), to support relevant research of the nation's best and brightest academic scholars in pursuit of homeland security related disciplines.** The HS-Centers program, which is operated by the Department's Science and Technology Directorate, is establishing an integrated network of university-based centers that will conduct multi-disciplinary research and develop innovative educational programs for critical Homeland Security missions. Through this program, Homeland Security and partner universities bring together the nation's best experts and **focus its most talented researchers on a variety of threats that include agricultural, chemical, biological, nuclear and radiological, explosive and cyber terrorism as well as the behavioral aspects of terrorism.**

Source: <http://www.dhs.gov/dhspublic/display?content=3517>

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

Emergency Services Sector

27. *April 27, Associated Press* — Interest growing in 'security' blimps. The horizon someday may be lined with giant floating orbs guarding people below from the enemy. **Such unmanned spherical airships that resemble giant golf balls could be used to protect areas from terrorists and missile attacks, watch weather developments and perhaps even provide wireless telephone service to developing nations.** Interest in airships has grown in recent years, with nearly 20 companies developing them in the United States and Europe. Now researchers are updating lighter-than-air technology for the 21st century with new power

systems and fabrics to help them survive the stratosphere's extreme temperatures and intense solar radiation. Floating about 13 miles above the earth and holding a stationary orbit for 12 to 18 months, they would provide more constant scrutiny than existing unmanned reconnaissance planes such as the medium–altitude Predator and the high–altitude Global Hawk that have to move around.

Source: <http://www.newsday.com/news/nationworld/wire/sns-ap-eyes-in-the-sky.0.361555.print.story?coll=sns-ap-nationworld-headlines>

28. *April 27, CTV (Canada)* — **New security policy to prevent terror attacks. Ottawa has announced a new national security policy aimed at improving passport control, port security, and intelligence gathering, as well as boosting Canada's ability to respond to national disasters and disease outbreaks.** The new initiatives will cost \$690 million over the next five years, with the funds coming from the Security Reserve and administered by Public Safety Minister Anne McLellan. The new policy is aimed at "protecting Canada and Canadians at home and abroad, ensuring Canada is not a base for threats to our allies and contributing to international security," McLellan said in a statement. **Six key areas are addressed in the new policy: intelligence, emergency management, public health, transportation, border security, and international security.**

Source: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1083072724092_4/?hub=TopStories

[[Return to top](#)]

Information Technology and Telecommunications Sector

29. *April 27, Federal Computer Week* — **DHS, NSA team on cybersecurity.** On April 22, officials from National Security Agency (NSA) and the Department of Homeland Security (DHS) announced the formation of the **National Centers of Academic Excellence in Information Assurance Education.** It stems from NSA's Centers of Academic Excellence in Information Assurance Education Program, which started in 1998 and recognizes 50 universities in 26 states. **The National Strategy to Secure Cyberspace, issued in 2002 by the Bush administration, directs the government to foster training and education programs that support computer security needs and responsibilities, and improve existing information assurance programs.** Earlier this month, NSA officials announced they would hire 1,500 people by September and 1,500 employees each year for the next five years. Agency jobs include information technology and acquisition positions in addition to traditional code–making and code–breaking roles, according to an April 7 statement.

Source: <http://fcw.com/fcw/articles/2004/0426/web-nsa-04-27-04.asp>

30. *April 26, IDG News Service* — **Attack code surfaces for recent MS security hole.** Computer code that claims to exploit a recently disclosed hole in Microsoft products has surfaced on a French–language Website. The code can be used by a remote attacker to trigger a buffer overrun vulnerability in the Local Security Authority Subsystem (LSASS). The code was released on Saturday, April 24, according to the Website. It was unclear whether the exploit code works, but notes attached by its author say some modifications may be necessary before the code can be used by a remote attacker to compromise Windows machines. **An attacker who could exploit the LSASS vulnerability could remotely attack and take total control of**

Windows 2000 and Windows XP systems, according to Microsoft. Unlike e-mail worms and viruses, no user interaction would be necessary to trigger the LSASS buffer overflow, according to Johannes Ullrich of the SANS Institute's Internet Storm Center. Microsoft released a patch for the LSASS vulnerability in Microsoft Security Bulletin MS04-011:

<http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx>

Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,92696,00.html>

31. *April 26, eSecurity Planet* — **'Critical' Windows hijack flaw reported. Security researchers have discovered a serious boundary error vulnerability in multiple versions of Microsoft's Windows platform and warned that attackers could hijack systems via Windows Explorer and Internet Explorer.** Rodrigo Gutierrez, a researcher with Trustix AS, notified Microsoft of the flaw with a warning that it could be exploited by malicious attackers to cause a buffer overflow and lead to system takeover. Microsoft confirmed Gutierrez's findings and recommended users install the latest service packs for Windows XP and Windows 2000. Independent security consultants **Secunia said the vulnerability "has been confirmed on fully patched systems running Windows XP and Windows 2000."** Secunia urged Windows XP and Windows 2000 users to restrict traffic in border routers and firewalls as a temporary workaround. Users could also disable the "Client for Microsoft Networks" for network cards to impact file sharing functionality. The flaw also reportedly affects Windows 95, 98, and Me. Secunia Advisory SA11482: <http://secunia.com/advisories/11482/>
Source: <http://www.esecurityplanet.com/alerts/article.php/3345351>
32. *April 26, Associated Press* — **SBC customers cut off from the Internet. Connecticut customers who use SBC Communications to reach the Internet were cut off from the World Wide Web much of Monday, April 26, after a fiber optic line was cut,** the company said. Beverly Levy, an SBC spokesperson, said the outage had cut service to customers who used SBC Dial-up or the DSL broadband service. Levy said that the vendor whose fiber line was cut Monday morning worked around the problem by routing Connecticut Internet traffic through New Jersey. By 3 p.m. customers had service restored, the company said.
Source: <http://www.stamfordadvocate.com/news/local/state/hc-26154805.apds.m0421.bc-ct-brf--apr26.0.7979178.story?coll=hc-headlines-local-wire>
33. *April 26, InformationWeek* — **Windows vulnerability exploited, worm may be next.** Security experts are monitoring widespread use of exploit code that takes advantage of a recently-disclosed vulnerability in Windows, but a worm, although anticipated, hasn't yet been spotted. The vulnerability stems from a flaw in Windows Protected Communications Technology (PCT) v. 1.0, a packet protocol within Microsoft's SSL library. An April bulletin from Microsoft warned that **an attacker could create a buffer overflow condition on vulnerable Windows servers, then follow that by inserting their own code into the system to take control. Windows XP and Windows Server 2003 systems are also vulnerable.** The first form of the exploit code was discovered within days of the disclosure of the SSL vulnerability, added Ken Dunham of iDefense. Last week, that code was updated to include a "phone home" feature that allowed hackers using it to be notified when they'd compromised a server. Additional information is available in Microsoft Knowledge Base Article 187498: <http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q187/4/98.asp&NoWebContent=1>
Source: <http://informationweek.securitypipeline.com/news/19201802.js>

34. *April 25, eWEEK* — **Feds making plans for security clearinghouse.** The federal government is developing plans for a secure network operations center (SOC) for all security information flowing to and from the government. The SOC would be a clearinghouse that gathers and analyzes data from the private sector, mainly the **Information Sharing and Analysis Centers (ISACS) in several major vertical industries.** The SOC would be run jointly by personnel from the DHS and a civilian contractor that would help build the facility. DHS officials said that even though there are less formal information-sharing efforts between government and private industry, there still is a need for a more structured program. "We're trying to operationalize the public/private partnership," said Amit Yoran, director of the National Cyber Security Division at DHS, last week. "The private sector genuinely wants to make progress on this. I think, as we get more considerate of the private sector in terms of the FOIA [Freedom of Information Act] exemption, things will come along." Officials said they hope to have plans for the SOC finalized soon and intend to fund the initiative out of the current fiscal year's budget, which runs out September 30.
 Source: <http://www.eweek.com/article2/0.1759.1572951.00.asp>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 3 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: HTML_NETSKY.P 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	445 (microsoft-ds), 137 (netbios-ns), 135 (epmap), 80 (www), 3127 (mydoom), 1433 (ms-sql-s), 1434 (ms-sql-m), 443 (https), 139 (netbios-ssn), 2745 (urbisnet) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

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

General Sector

35. *April 28, Reuters* — **U.S. concerned al Qaeda will try to attack this year.** The U.S. government is concerned al Qaeda will try to launch an attack on American soil this year with high-profile events such as the presidential election approaching, John Brennan, director of the Terrorist Threat Integration Center (TTIC), said on Monday, April 26. The train bombings in Madrid in March, followed within days by the election ouster of the pro-American governing

party, and a half dozen broadcasts from al Qaeda leader Osama bin Laden and his deputy Ayman al-Zawahri since the fall promising attacks against U.S. interests, has fueled those concerns. **"If in fact some folks believe that they can affect elections with terrorism, this is something that we need to be very vigilant about," Brennan said.** The timing for al Qaeda attacks is usually tied to when the plot is ready, but U.S. authorities are taking the view that such high-profile events as the November presidential election may be factors considered by the extremist group, he said. The center, which reports to the director of central intelligence, currently has 76 analysts from the CIA, FBI, Department of Defense, Department of State, Department of Homeland Security, and other agencies.

Source: [http://www.nytimes.com/reuters/news/news-security-threats.ht ml](http://www.nytimes.com/reuters/news/news-security-threats.html)

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

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, 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: Send mail to dhsdailyreport@mail.dhs.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644.

Subscription and Distribution Information: Send mail to dhsdailyreport@mail.dhs.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at info@us-cert.gov or visit their Web page at www.uscert.gov.

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.