

Department of Homeland Security
Information Analysis and Infrastructure
Protection
Daily Open Source Infrastructure Report
for 14 July 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- The New York Times reports officials have announced the indictment of 24 people who they say were part of a theft ring that plundered millions of dollars in goods from freight trains over the past decade. (See item [10](#))
- The Associated Press reports police said Thursday that a French high school student is being investigated on suspicion of breaking into and defacing some 2,000 Web sites in France, Britain, Australia and the United States. (See item [25](#))
- internetnews.com reports the Apache Software Foundation on Monday released a new version of its open-source Web server project to plug four potentially serious security holes. (See item [28](#))

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: Elevated, Cyber: Elevated

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

1. *July 11, Reuters* — **Nuclear material in transit vulnerable to attack. Despite stepped-up security after September 11, 2001, countries remain ill prepared to deal with attacks on nuclear materials in transit, participants at a United Nations conference said.** The U.N. International Atomic Energy Agency (IAEA) says radioactive materials ranging from harmless medical supplies to weapons-grade plutonium account for less than two percent of all goods transported by land, 10 percent by air and one percent by sea. **But the volumes are still huge. The cargo carrier DHL boasts on a company brochure that it transports five tons of radioactive material per week on 113 aircraft to 40 destinations around the globe.** While

acknowledging there was reason for some concern about the security risks of transporting nuclear materials, IAEA chief Mohamed ElBaradei told a week-long conference on the issue that international regulations and industry practice have "an excellent safety record." But John H. Large, a consultant on nuclear issues hired by the environmental group Greenpeace, said current emergency plans would only work for "unintelligent accidents." **"What they haven't prepared for is an intelligent terrorist attack where they know the vulnerabilities of your emergency plan," Large told Reuters.** For example, he said it would be easy to take a rocket-propelled grenade and shoot it at a standard transport vehicle loaded with radioactive fuel.

Source: <http://www.nytimes.com/reuters/news/news-nuclear-crime.html>

2. *July 10, Akron Beacon Journal, Ohio* — **Akron, Ohio-based FirstEnergy eyes August for restart of nuclear power plant.** FirstEnergy Corp. may know next week if its Davis-Besse nuclear power plant will be ready to restart before the end of summer. **Modifications to crucial Davis-Besse safety equipment, two high pressure injection (HPI) pumps that would keep the nuclear fuel cool in the event of a major accident, have yet to pass all tests to show that they will not clog and break during an emergency, FirstEnergy and Davis-Besse executives told a Nuclear Regulatory Commission oversight panel on Wednesday.** If the modifications don't pass, then the Akron utility is faced with additional delays by having to replace the massive pumps with new ones that it already bought as a precaution. The most recent tests using mockups show that insulation fiber mixed in reactor coolant can clog the modified pumps in as little as 15 minutes, the executives said during a meeting at Oak Harbor High School. The tests are designed to simulate a loss of coolant accident inside the containment chamber, which could blow loose insulation, concrete and metal pieces and possibly damage safety equipment. **The NRC oversight panel has a checklist of 31 items that must be completed and passed before Davis-Besse will be allowed to restart.**

Source: http://www.energycentral.com/sections/news/nw_article.cfm?id=3980054

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

Chemical Sector

Nothing to report.

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

Defense Industrial Base Sector

3. *July 10, U.S. Department of Defense* — **DCIS agents launch 18-company search in tech transfer case.** Joseph E. Schmitz, Department of Defense Inspector General, announced today that agents from the Defense Criminal Investigative Service (DCIS) and the Bureau of Immigration and Customs Enforcement (ICE) **executed search warrants on 18 U.S. companies in ten states as part of an ongoing investigation regarding illegal transfer of military components in violation of the Arms Export Control Act.** **DCIS agents, working with Department of Homeland Security ICE agents, launched a multi-state execution of search warrants in Colorado, Florida, Kansas, Louisiana, New Hampshire, New York, Oregon, South Carolina, Texas, and Wisconsin.** Additionally, DCIS and ICE agents served a

total of eight subpoenas and conducted one "consent search." Each of the firms is suspected of exporting military technology on the U.S. Munitions List without obtaining the appropriate license from the U.S. Department of State. **Among the military technology allegedly included in the exports were components for the F-4 Phantom, F-5 Tiger and F-14 Tomcat aircraft, and the Hawk Missile System. The companies allegedly shipped these components to a London-based company, Multicore, LTD., which also operated under the name AKS Industries.** U.S. authorities found that Multicore London has ties to the Iranian military.

Source: <http://www.dod.mil/releases/2003/nr20030710-0188.html>

4. *July 10, Federal Computer Week* — **Dept. of Defense opens biometrics site.** The Defense Department's Biometrics Fusion Center announced that its DoD Biometrics Knowledgebase System is now open to all government personnel. The Web site, protected by Secure Sockets Layer, became accessible to all government users with .gov or .mil addresses on June 30. **The site is DoD's primary authoritative source of information on biometric test and evaluation methods and reports, enterprise working group progress, biometrics policy and strategic direction, and biometric program implementation plans and schedules.** Army Maj. Stephen Ferrell, the center's director, said the site should be used "for the exchange of information between the DoD biometrics program community and DoD establishment at large." The Biometrics Senior Coordinating Group and Biometrics Enterprise Working Groups began using the first iteration of the system February 3. Biometrics Fusion Center personnel have been fine-tuning the site's technical elements since then to incorporate user feedback and publish the initial stages of device testing and evaluation methods, Ferrell said. **The Biometrics Knowledgebase System features biometric overviews, frequently asked questions, tutorials, and details of different DoD testing methods, including outlines of proprietary report data from Biometrics Fusion Center evaluations.**

Source: <http://www.fcw.com/fcw/articles/2003/0707/web-dodbio-07-10-03.asp>

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

Banking and Finance Sector

5. *July 11, Washington Post* — **Immigrants turn to Salvadoran banks for money transfers .** Elio Hernandez, a 32-year-old maintenance worker who moved to the District from El Salvador three years ago, walked into Banagricola, a tiny storefront money-transfer operation in Adams Morgan, and paid \$10 to send \$60 to his 80-year-old grandmother and his two children in San Salvador. Hernandez said he uses Banagricola because it is a subsidiary of Banco Agrícola, which is the largest bank in his home country. Its 513 branches in El Salvador make it easy for his grandmother to get the money. "I prefer to use a Salvadoran bank," Hernandez said in Spanish. "It's more convenient for my family." **Such connections with the Salvadoran immigrant community have made Banagricola and its local competitor, Banco de Comercio—El Salvador's fourth-largest bank and the parent company of Bancomercio money-transfer centers—significant players in the Washington area's money-transfer market. Both Banagricola—whose motto is "El Salvador much closer to you"—and Bancomercio have storefront money-transfer businesses nestled amid fast-food restaurants and check-cashing stores in commercial strips in Hispanic enclaves.**

Source: http://www.washingtonpost.com/wp-dyn/articles/A40585-2003Jul_10.html

Transportation Sector

6. *July 11, sunspot.net* — **New boats to aid city officers with homeland security. In an upgrade for Baltimore police, city officers are now patrolling Baltimore's waterways in a sophisticated boat that they say will play a crucial role in homeland security.** "It's great," said Lt. Gabe Bittner, commander of the marine unit. "It's the newest technology out there. It enables us to protect the harbor, protect the city against terrorism also while performing our normal patrol functions." **The \$143,000 27-foot SeaArk craft, which arrived two weeks ago, is packed with radar, sonar and a satellite navigation system. It soon will be outfitted with surveillance cameras that can beam images to police officials, who could be making crucial decisions during a crisis.** The boat has twin 225-horsepower outboard engines – it can travel up to 50 mph – and smoothly skims across choppy waters at high speeds. **The craft will be joined this summer by two more SeaArks, a 36-footer and a 25-footer—all financed by a \$550,000 federal grant.**

Source: <http://www.sunspot.net/news/local/bal-md.boat07jul07.0.4344844.story?coll=bal-local-headlines>

7. *July 11, Government Computer News* — **FAA commissions an enhanced GPS system. The Federal Aviation Administration's latest modernization component, one designed to help pilots land safely, officially went into operation Thursday. The Wide Area Augmentation System, or WAAS, was commissioned at David J. Hurley Air Traffic Control Systems Command Center in Herndon, VA, after years of cost overruns and delays.** WAAS will be available at 280 airports. Small and general aviation carriers will benefit the most from the satellite system, although commercial carriers also can use WAAS, an FAA spokeswoman said. Large commercial carriers use the satellite-based Global Positioning System.

Source: http://www.gcn.com/vol1_no1/daily-updates/22728-1.html

8. *July 10, vnunet.com* — **UK airports put the finger on asylum seekers. Trials of biometric security checks are to begin next month, as the government attempts to cut fraudulent immigration and asylum claims.** Sri Lankan nationals asking for UK visas will be fingerprinted in their home country when they apply. Readers installed at British airports will then match individuals to the visa. Immigrations officials and other law enforcement agencies will be able to access this information to help them identify claimants, according to a Home Office spokesman. The system is aimed at reducing bogus applications, where claimants have either made applications under a false name or attempted to frustrate repatriation by destroying documents. **Sri Lanka has been selected for the pilot because the Home Office has identified a "significant number of unfounded applications" originating in the country. The spokesman confirmed that fingerprint scanners will be installed at points of entry in time for the trial to begin next month.** Biometric testing has been placed at the heart of government plans to tackle bogus asylum applications. "Using cutting edge technology to help secure our borders will ease travel for legitimate passengers, but allow us to stop and deter those who have no right to be here," said Home Office minister Beverley Hughes in a statement. In similar trials, iris scanners are being installed at 10 UK airports by the middle of next year.

Source: <http://www.vnunet.com/News/1142170>

9. *July 10, Associated Press* — **Better air maintenance oversight urged. The Federal Aviation Administration does not adequately oversee the growing number of outside contractors repairing commercial airplanes, the Transportation Department's inspector general said Thursday. At 18 of 21 facilities checked by government investigators, contract mechanics used incorrect aircraft parts and improperly calibrated tools and had outdated manuals.** "The vulnerabilities all relate to a lack of effective FAA oversight that needs to be improved," the report said. FAA Administrator Marion Blakey said the agency agrees with the findings. However, she stressed the report does not say passengers are in any danger. **Air Midwest, operating as US Airways Express, used an outside contractor to maintain the commuter plane that crashed on takeoff at North Carolina's Charlotte–Douglas International Airport in January, killing all 21 aboard.** The ongoing investigation found a mechanic could have improperly set turnbuckles, which control tension on elevator control cables. If a cable is too slack, the pilot does not have full control of the elevator, a tail flap that moves up and down and causes the plane to climb or dive.

Source: http://www.washingtonpost.com/wp-dyn/articles/A40316-2003Jul_10.html

10. *July 10, New York Times* — **24 are indicted in ring that looted cargo trains.** State officials today (July 10) announced the indictment of 24 people who they say were part of a theft ring that plundered millions of dollars in goods from freight trains over the past decade. **According to the 38-count indictment, members of the group, which called itself the "Conrail Boyz," would leap onto the slow-moving trains coming into and out of Croxton Terminal in Jersey City and use bolt cutters to break into cargo containers full of electronics, clothing, cigarettes and other items.** They would throw boxes of goods off the trains to accomplices, who would load them into trucks and ferry them away, according to investigators. The indictments grew out of a two-year investigation during which state law enforcement authorities and the Norfolk Southern Railroad police followed the group's activities from theft to resale of the items. **In the process, investigators developed a picture of a "sophisticated cartel" involved in money laundering. The operation mimicked corporations, the investigators said, and had an international reputation for dealing in a wide variety of black-market items.**

Source: <http://www.nytimes.com/2003/07/11/nyregion/11CARG.html>

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

11. *July 11, New York Times* — **Canada pushes hard to end ban on cattle exports.** Nearly two months after the carcass of a single cow tested positive for bovine spongiform encephalopathy, or mad cow disease, Canada has started a desperate diplomatic campaign to reopen

international markets to its cattle industry. **After slaughtering more than 2,000 cows in three provinces, animal health experts said they had found no evidence that the infection had ever entered the food supply. Still, more than 30 countries have banned Canadian beef, in part because authorities have not been able to determine conclusively how a single cow on a remote ranch in northern Alberta contracted the disease.** Canada's beef industry is losing about \$8 million a day because of the bans. In recent days, Prime Minister Jean Chrétien has telephoned President Bush and Prime Minister Junichiro Koizumi of Japan to try to convince them that Canadian beef is safe. President Bush told Chrétien that he would press for a rapid reopening of the American market, which normally takes nearly 80 percent of Canada's beef exports, or \$2.5 billion worth a year. **But United States officials say their hands are virtually tied, because America's own largest export market for beef, Japan, has said it may block shipments unless they are certified free of beef from Canada.**

Source: <http://www.nytimes.com/2003/07/11/business/worldbusiness/11MEAT.html>

12. *July 11, Reuters* — **Feed maker admits to mad cow violation. The U.S. Food and Drug Administration (FDA) said on Friday a Washington state livestock feed manufacturer admitted to selling "adulterated and misbranded" feed that violated federal rules to prevent mad cow disease.** The FDA reiterated that the United States has never had a case of mad cow disease. X-cel Feeds Inc. was ordered to adopt clean-out procedures at its plant, obtain protein supplier certifications and take other measures to comply with FDA rules, the agency said. **The FDA said it filed a permanent court injunction against X-Cel for "introducing adulterated and misbranded animal feeds into interstate commerce."** **However, an FDA spokesman was not immediately available to clarify if that meant X-Cel's manufacturing plant would be permanently closed.**

Source: <http://asia.reuters.com/newsArticle.jhtml?type=scienceNews&storyID=3076912>

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

Food Sector

13. *July 11, AgWeb* — **USDA releases food safety plan. The U.S. Department of Agriculture (USDA) has released a food safety vision entitled "Enhancing Public Health: Strategies for the Future," that will guide continuing efforts to improve the safety of U.S. meat, poultry, and egg products and protect public health.** The Food Safety and Inspection Service (FSIS) is working to lessen the time between the development and implementation of new technologies that will improve meat and poultry safety. **FSIS will be conducting baseline studies to determine the nationwide levels of various pathogenic microorganisms in raw meat and poultry.** FSIS is working with the Research, Education, and Extension mission area at USDA to coordinate food safety research priorities and needs. The research agenda will include a mechanism by which research needs in food safety are prioritized. **FSIS will retool its education and training programs so that its workforce is better prepared to implement and enforce new food safety regulations.** In consultation with livestock producers, researchers and other stakeholders, FSIS is developing a list of best management practices for animal production facilities such as feedlots to provide guidance in reducing pathogen loads before slaughter. The complete document can be found at

<http://www.fsis.usda.gov/oa/programs/vision071003.htm>

Source: http://www.agweb.com/news_show_news_article.asp?file=AgNewsA

[[Return to top](#)]

Water Sector

14. *July 11, Water Tech Online* — EPA awards \$700,000 grant for drinking water protection. **Officials from the U.S. Environmental Protection Agency (EPA) presented a \$700,000 grant July 2 to the Upper Susquehanna Coalition as part of a new EPA national initiative supporting community-based approaches to cleaning up the nation's watersheds.** The Upper Susquehanna watershed, a 7,534 square-mile largely agricultural area that stretches from Otsego, NY, to Athens, PA, is home to 100,000 people. Mark Watts, district manager of the Chemung County Soil and Water Conservation District and chairperson of the Upper Susquehanna Coalition said, "This funding will support our efforts at the county level to address local water quality issues of importance while also having positive benefits to our downstream neighbors."

Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=41610

15. *July 10, Scripps Howard News Service* — **Most states predict water shortages in next decade. Water managers in most states expect shortages of freshwater in the next decade, and the consequences may be severe, according to a General Accounting Office (GAO) report released Thursday.** National water availability and use has not been comprehensively assessed in 25 years, but current trends indicate that demand on the nation's water supply is growing, said the accounting office. **The nation's capacity for building new dams and reservoirs to store surface water is limited, and groundwater in many parts of the country is being depleted faster than it can be replenished,** the report said. At the same time, the GAO reported, a growing population and increased pressure to allocate water to fisheries and the environment are placing new demands on the freshwater supply. **As a result, water managers in 36 states surveyed by the GAO said they anticipate water shortages in the next 10 years under "average water conditions."** There have been eight water shortages resulting from drought or heat waves over the past 20 years resulting in more than \$1 billion in damages each, the report said. The most costly totaled over \$40 billion in damages to the economies of the central and eastern United States in the summer of 1988. The report can be found at <http://www.gao.gov/new.items/d03514.pdf>.

Source: <http://www.knoxstudio.com/shns/story.cfm?pk=WATERSTATES-07-10-03&cat=AN>

[[Return to top](#)]

Public Health Sector

16. *July 11, Associated Press* — **Nine held in Texas on SARS concerns. Nine people connected to the military have been quarantined in Texas after some reported respiratory problems similar to Severe Acute Respiratory Syndrome (SARS), officials said.** A Group of military personnel passed through the Toronto Airport recently, and some reported mild to moderate respiratory problems earlier this week after returning home, said Capt. David May of Dyess Air

Force Base in Abilene. **Only one person in the group fits the definition of a suspected SARS case, and no one has been officially diagnosed with SARS or been hospitalized, May said. But he said the military travelers and some people they've come in contact with, nine people in all, are now under home quarantine.** Officials with the Abilene–Taylor County Public Health District said Thursday that there is no reason for alarm.

Source: <http://www.msnbc.com/news/937648.asp?0cv=HA00>

17. *July 10, Reuters* — **France ill–equipped for bioterror attacks. France is one of the countries least prepared against bioterrorist attacks and should draw up a national plan to combat diseases that could be unleashed against its people, an official report said on Wednesday.** The report for the health and research ministries described possible terror attacks with biological weapons as a real danger that the French government has not taken seriously enough. "The country has shown in recent years a limited ability to deal with the problem of infectious diseases, which means it is one of the least prepared for the problem of a massive epidemic," the report said. **France should set up a national network of disease control centres, similar to that in the United States, to prepare hospitals for potential health emergencies due to highly contagious diseases, it said.**

Source: <http://www.alertnet.org/thenews/newsdesk/L09677610.htm>

18. *July 10, Government Technology* — **Delaware to safeguard against bioterrorism. Delaware is embarking on becoming the first state in the nation to provide statewide electronic access to clinical information at the point of care.** A key to the system is that patient consent is required and access is strictly limited to the provider delivering the care. The first phase of implementation is expected to be in place within six months, followed by a more robust clinical data sharing capability that will facilitate the reduction of medical errors, improve quality and reduce health care costs. **"The system will also provide state health officials with an enhanced capability to identify the first signs of a bioterrorism attack or a new infectious disease like SARS,"** said Lt. Gov. John C. Carney, Jr. At least one private consulting firm estimated that the new system could save \$40 billion a year in health care costs if implemented nationally.

Source: <http://www.govtech.net/news/news.php?id=2003.07.10-59373>

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

Government Sector

19. *July 11, U.S. Department of Homeland Security* — **Regulations implementing the Support Anti–Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) proposed rule.** The SAFETY Act, through regulations promulgated by the Department of Homeland Security, will provide critical incentives for the development and deployment of anti–terrorism technologies by providing liability protections for Sellers of "qualified anti–terrorism technologies" and others. **The Department of Homeland Security intends to implement the SAFETY Act as quickly as possible. The Department does not intend to resolve every conceivable programmatic issue through this proposed rule. Instead, the Department will set out a basic set of regulations and commence the implementation of the SAFETY Act program while considering possible supplemental regulations as experience with the Act grows.** After reviewing the comments, the Department may issue an

interim final rule and seek additional comment on some or all aspects of the program. In any event, the Department will begin implementation of the SAFETY Act immediately with regard to Federal acquisitions of anti-terrorism technologies and will begin accepting other SAFETY Act applications on September 1, 2003.

Source: <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-17561.htm>

20. *July 11, Christian Science Monitor* — **Terror threat raises U.S. interest in Africa. The September 11 terrorist attacks have increased the global significance of Africa, with its poverty, failed states, mineral wealth, and 250 million Muslims, making the continent a potential haven and source of funding for groups like al Qaeda.** Since 1998, there have been four attacks in Africa, including one late last year in Kenya, believed to have been organized by al Qaeda or associated groups, costing almost 300 lives. Countries like Sudan and Somalia are reported to have sheltered the terror organization's members, while diamonds from places like Liberia and Sierra Leone may have been used to fund its operations. And just last month, five men with alleged ties to al Qaeda were arrested in Malawi. **President Bush has pledged \$100 million to help East African countries improve their counterterrorism efforts, including border security – most of those arrested in recent terror attacks are non-Africans. Since late last year, the US has had 1,800 troops in Djibouti conducting counterterrorism operations.**

Source: <http://www.csmonitor.com/2003/0711/p08s01-woaf.html>

21. *July 11, Associated Press* — **Officials criticize new visa regulation. On Thursday, tourism officials painted a bleak picture of long lines at U.S. embassies, frustrated foreigners who have to wait months to get a visa to visit America, millions in lost revenue.** "The increase in interviews will cost the U.S. travel and tourism industry hundreds of millions of dollars and thousands of lost jobs," John Marks, chairman of the Travel Industry Association of America, told the House Government Reform Committee. **For years the United States has required foreigners seeking non-immigrant visas to appear for personal interviews, but consuls abroad had been granted wide discretion to waive the requirement, said Janice Jacobs, deputy assistant secretary of state for visa services. Beginning August 1, the State Department is tightening the conditions under which waivers can be granted.**

Source: http://www.washingtonpost.com/wp-dyn/articles/A40035-2003Jul_10.html

22. *July 11, Reuters* — **Bush press plane stowaway raises security scare.** A stowaway flew from South Africa to Uganda on the press plane accompanying President Bush on his visit to Africa and entered the compound where Bush met Uganda's president, U.S. officials said. **U.S. Secret Service agents conducted a security sweep on the plane after the unidentified stowaway was detained and removed from the compound on the shores of Lake Victoria where Bush met President Yoweri Museveni Friday. "He did not have a credential. He did not have a passport. He has nothing," said White House travel office official Curtis Jablonka.** He said the chartered United Airlines Boeing 747 carrying about 130 members of the press, White House staff and Secret Service agents had been "thoroughly swept." The Secret Service typically provides security oversight for the delegation. "There was no indication the stowaway came within sight of President Bush," Jablonka added.

Source: http://www.publicbroadcasting.net/wxxi/news.newsmain?action=article&ARTICLE_ID=520484

23. *July 10, Federal Communications Commission* — **FCC establishes Office of Homeland Security.** The Federal Communications Commission (FCC) on Thursday announced the creation of an Office of Homeland Security (Office) within the Enforcement Bureau. The new Office will provide consolidated support for the homeland security and emergency preparedness responsibilities of the Commission and the Defense Commissioner (currently, Chairman Powell), the agency's Homeland Security Policy Council, and the Chief, Enforcement Bureau. James A. Dailey, a 31-year FCC veteran, has been named Director of the Office. **The Office will be responsible for rulemaking proceedings relating to the Emergency Alert System and will oversee operation of the Commission's 24-hour Communications and Crisis Management Center and its Emergency Operations Center, functions that are currently handled in the Enforcement Bureau's Technical and Public Safety Division.** FCC Homeland Security Action Plan:

http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-236429_A1.pdf Powerpoint

presentation: http://www.fcc.gov/hspc/presentation_071003.pdf

Source: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-236436_A1.pdf

[[Return to top](#)]

Emergency Services Sector

24. *July 13, New York Daily News* — **Online army takes on terror.** The New York City Police Department has a cadre of investigators of Middle Eastern or Asian descent fluent in foreign languages who work in the Intelligence Division's cyber unit. Formed 18 months ago, the unit has compiled millions of records in its database and culls through thousands of E-mails a day. Police Commissioner Raymond Kelly and the deputy commissioner for intelligence, David Cohen, a former CIA spymaster, has cloaked the division in a measure of mystique, but the Daily News was given an inside look at Intel's headquarters. **The division investigates about 35 terrorism hotline tips a day – as many as 200 when the nation goes on high alert. It recently launched the petty crime initiative, which concentrates on economic crimes that fund terrorism: cigarette-tax evasion, product counterfeiters, money orders, petty larceny, credit card schemes. Such crimes generate millions of dollars in a few months, and investigators try to connect the dots to known terrorist organizations.**

Source: <http://www.nydailynews.com/front/story/100324p-90717c.html>

[[Return to top](#)]

Information and Telecommunications Sector

25. *July 10, Associated Press* — **Teenage hacker suspected of violating 2,000 sites.** A French high school student is being investigated on suspicion of breaking into and defacing some 2,000 Web sites police said Thursday. The 17-year-old boy, who went by the pseudonym "DKD," hacked into sites and often replaced their welcome pages with political slogans, said Eric Voulleminot of the Regional Service of Judicial Police in Lille, France. **The teenager is accused of attacking sites in France, Britain, Australia and the United States, Voulleminot said. The boy allegedly concentrated on government office and military sites, including**

that of the U.S. Navy. Suspected of attacks over 14 months, he was arrested June 24 at his parents' home outside of Paris and released under surveillance. **Investigators think his goal was showing off technical skill rather than spreading a political message.** The suspect faces a maximum sentence of three years in prison and a fine \$50,850.

Source: http://www.usatoday.com/tech/news/computersecurity/2003-07-10-script-kiddie_x.htm

26. *July 10, PostNewsweek Tech Media* — **Cybersecurity laws coming, Putnam says.**

Cybersecurity regulation that will affect the private sector is on the way this year, Rep. Adam Putnam (R-FL) said Thursday at a Capitol Hill forum sponsored by the Business Software Alliance and the Center for Strategic and International Studies of Washington. Business Software Alliance president Robert W. Holleyman argued against regulation. **"The government must avoid mandates and allow the private sector to develop and deploy security technology in partnership with it,"** Holleyman said. **But companies "have not moved fast enough. It is incumbent on the private sector to get its house in order to demonstrate that regulation is not needed,"** Putnam said.

Source: <http://www.washingtontechnology.com/cgi-bin/udt/im.author.contact.view?client.id=wtdaily-test&story.id=21167>

27. *July 09, Washington Technology* — **NIST: Security products need standardization. Despite wide use across government, intrusion detection systems have no standard metrics to measure their performance, according to a new report by the National Institute of Standards and Technology.**

The report "An Overview of Issues in Testing Intrusion Detection Systems" concluded that **there are no comprehensive and scientifically rigorous methodologies to test the effectiveness of intrusion detection systems,** which monitor and analyze systems and network traffic for possible hacker attackers or misuse. The report may be viewed here: <http://csrc.nist.gov/publications/nistir/>.

Source: <http://www.securityfocus.com/news/6327>

28. *July 09, internetnews.com* — **DoS holes plugged in Apache HTTP Server. The Apache Software Foundation on Monday released a new version of its open-source Web server project to plug four potentially serious security holes.**

The latest update to the Apache 2.0 HTTP Server (version 2.0.47) is described as a security and bug fix release to plug holes that could lead to denial-of-service attacks. The Foundation warned that **the SSLCipherSuite directive being used to upgrade from a weak ciphersuite to a strong one could result in the weak ciphersuite being used in place of the strong one. The previous Apache HTTP Server version also contains a bug in the prefork MPM** where certain errors returned by accept() on rarely accessed ports could cause temporal DoS. **Another DoS security vulnerability, caused when target host is IPv6, was also patched.** Apache explained that ftp proxy server can't create IPv6 socket. The Apache Foundation also warned older versions of the server would crash when going into an infinite loop because of too many subsequent internal redirects and nested subrequests.

Source: <http://www.internetnews.com/infra/article.php/2232981>

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

[[Return to top](#)]

General Sector

29. July 12, Reuters — Indonesian police arrest nine in Bali attacks. The Indonesian police, acting during the past week in several different locations, have arrested nine suspected Jemaah Islamiyah militants linked to the attacks in Bali last year and have seized explosives and bomb-making chemicals. **One suspect arrested in the Jakarta area was Pranata Yuda, also called Mustofa, 42, whom the police identified as Jemaah Islamiyah's former chief for a region that incorporates parts of eastern Indonesia, Malaysia and the southern Philippines. Officials said papers indicating new targets had also been found. But officials denied rumors that they had caught Jemaah Islamiyah's suspected operations chief, known as Hambali, who is believed to be a link to al Qaeda.** Jemaah Islamiyah has been blamed for the bomb attacks in Bali in October, which killed more than 200 people, as well as other bombings in Southeast Asia.

Source: <http://www.nytimes.com/2003/07/12/international/asia/12INDO.html>

30. July 10, Arizona Republic — Al Qaeda target: Western forests. National forests in the West were considered targets for al Qaeda attacks. **A senior al Qaeda detainee told federal investigators he had developed a plan to set midsummer forest fires in Colorado, Montana, Utah and Wyoming, according to the document, obtained by The Arizona Republic.** The unidentified detainee said he hoped to create several large, catastrophic wildfires at once, mimicking the destructive fires that swept across Australia in 2002, according to the memo. **"It goes along with the rest of the alerts," said Rose Davis, a spokeswoman for the National Interagency Fire Center in Boise, ID. "It's a reminder to be vigilant. We hope the public is, too. If you see something suspicious in an airport, report it. Likewise, if you see something suspicious in a forest, report it."**

Source: <http://www.azcentral.com/news/articles/0710forestterror-ON.h tml>

[[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: 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.