Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 28 April 2005

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
http://www.dhs.gov/

Daily Highlights

- Knight Ridder Tribune reports the Texas Department of Public Safety mailed hundreds of Texas driver's licenses to the wrong people, due to a malfunctioning machine that was recently installed to sort licenses for mailing. (See item 5)
- The Associated Press reports the Arizona Minuteman civilian patrol group that has been monitoring the Mexican border for illegal immigrants is planning to expand its mission to the Canadian border. (See item 10)
- The US−CERT has released "Technical Cyber Security Alert TA05−117A: Oracle Products Contain Multiple Vulnerabilities." (See item 23)

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, Brascan Power* — **Brascan Power acquires hydroelectric plants in eastern United States.** Ontario, Canada−based Brascan Power announced on Wednesday, April 27, that it has completed the acquisition of two hydroelectric generating stations totaling 48 megawatts of capacity from Reliant Energy for US$42 million. "The closing of this acquisition is a significant milestone in our strategy to expand in the northeast as it marks our first foray into the Pennsylvania, New Jersey and Maryland (PJM) electricity market. At the same time, it

furthers our objective of geographic diversification," said Harry Goldgut, Chairman and Chief Executive Officer of Brascan Power. The Piney station is a 28 megawatt facility located on the Clarion River in Pennsylvania and the Deep Creek station is a 20 megawatt facility located on the Youghiogheny River in Maryland.
Source: http://biz.yahoo.com/bw/050427/275815.html?.v=1

2. *April 26, Associated Press* — **Sea lion trapped in power plant intake tank.** A 300−pound sea lion has been living in the water intake tank of a power plant dodging rescue attempts since last week, the Los Angeles Department of Water and Power (DWP) said Tuesday, April 26. The male sea lion squeezed through an opening of the tank at DWP's fossil fuel plant in Playa del Rey, said spokesperson Darlene Battle. The sea lion became trapped April 18 after it swam through a pipe that feeds into the Pacific Ocean and squeezed through a gap in a fence designed to keep out large sea mammals, Battle said. Water in the 60−foot by 30−foot tank is used to cool plant generators. Battle said DWP enlisted the help of the nonprofit marine animal rescue group, Whale Rescue Team. Team members lowered a boat containing a cargo net into the tank, but the sea lion has avoided the rescue net that crews hoped to use to lift the animal, she said. DWP provides water and electricity to about 3.8 million residents and businesses in Los Angeles.
Source: http://www.signonsandiego.com/news/state/20050426−2019−ca−tr appedsealion.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *April 27, Government Accountability Office* — **GAO−05−631T: Homeland Security: Federal and Industry Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Action Is Needed (Testimony).** Terrorist attacks on chemical facilities could severely damage the U.S. economy and public health. About 15,000 facilities produce, use, or store large amounts of chemicals that pose the greatest risk to human health and the environment. While the Environmental Protection Agency (EPA) formerly had the lead role in federal efforts to ensure chemical facility security, the Department of Homeland Security (DHS) is now the lead federal agency responsible for coordinating government and private efforts to protect these facilities from terrorist attacks. This testimony is based on the Government Accountability Office's (GAO) past work on chemical facility security and focuses on (1) the attractiveness of chemical facilities as terrorist targets, (2) their diversity and risks, (3) federal security requirements for these facilities, and (4) federal and industry efforts to improve facility security. In March 2003, GAO recommended that DHS and EPA develop (1) a comprehensive chemical security strategy and (2) a legislative proposal to require facilities to assess their vulnerability to attacks and require corrective action. At that time, DHS and EPA generally agreed with these recommendations and, while EPA no longer has a key role in ensuring chemical facility security, DHS is taking steps to implement them. Highlights: http://www.gao.gov/highlights/d05631thigh.pdf
Source: http://www.gao.gov/new.items/d05631t.pdf

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *April 26, Associated Press* — **Federal agencies give banks guidance on risk.** Banks are receiving guidance to help them better gauge whether check cashers, money transmitters and other people who use their services may be vulnerable to money−launderers or terrorist financiers. The federal regulators' guidance, issued Tuesday, April 26, is aimed at resolving the problem of some check cashers, money transmitters and others being cut off from banking services. Some banks are closing the accounts of such money−services businesses out of fear they might run afoul of regulations designed to catch money−launderers and terrorist financiers. Banks as well as money−services businesses have asked federal regulators for help. The regulatory guidance makes clear that not all money−services businesses pose the same level of risk and that banks should tailor their due diligence accordingly. The guidance was issued by the Financial Crimes Enforcement Network (FinCEN), Federal Reserve, Federal Deposit Insurance Corp., Office of the Comptroller of the Currency, Office of Thrift Supervision and the National Credit Union Administration. FinCEN also provided guidance to money−services businesses. They stressed that such businesses that fail to take basic steps such as registering with federal authorities or complying with state licensing requirements may face regulatory action by the government and could lose access to their bank account.
   Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States: http://www.fincen.gov/guidance04262005.pdf
   Advisory to Money Service Businesses: http://www.fincen.gov/fincenadv04262005.pdf
   Source: http://biz.yahoo.com/ap/050426/banking_access.html?.v=1

5. *April 26, Knight Ridder Tribune* — **Hundreds of Texas driver's licenses mailed to wrong people.** An agency that warns Texans not to share personal information with strangers because of the risks of identity theft mistakenly mailed hundreds of driver's licenses to the wrong people. The Texas Department of Public Safety (DPS) blamed the mix−up on a malfunctioning machine that was recently installed to sort licenses for mailing. Statewide, at least 500 to 600 people who applied for a license renewal or replacement in late March or early April instead received somebody else's card, said DPS spokesperson Tela Mange. A driver's license contains enough personal information for thieves to open up a line of credit or a bank account in that name, make long−distance phone calls or apply for a Social Security card, according to the Texas attorney general's office. Information on the license includes a full name, signature, birth date, height, eye color, address and a photograph. The driver's license number, assigned by DPS, is also used by many agencies to verify a person's identity. In the case of the mismailed licenses, no identity theft or other crime has been reported, Mange said.
   Source: http://www.kansascity.com/mld/kansascity/news/nation/1149717 5.htm

6. *April 26, TechWeb News* — **Phishers play off Google.com.** Spyware authors and phishing scammers are using an old technique to draw unsuspecting users: Websites purposefully designed to take advantage of typing errors. Finnish security firm F−Secure has discovered a

site just one letter different than Google.com that when accidentally visited, drops a slew of malicious software on users' PCs. The site and several affiliated sites are registered to various Russian nationals, said F−Secure. Visitors who stumble on the site by mistyping google.com are immediately presented with two pop−up windows linked to sites that in turn load executable files exploiting several Windows vulnerabilities. By the time the entire episode's over, the machine has been infected with two backdoor components, two Trojans that drop a pair of DLLs onto Windows, a proxy Trojan, a Trojan−style piece of spying that steals bank−related information, and a Trojan downloader that can retrieve and install yet more malware. “The entire model for phishers is to re−route people to malicious Websites," said Avivah Litan, research director with Gartner, an IT industry research and analysis company. "They've been using this technique for the last 18 months or so. It's definitely primitive −− most phishers have gone on to more sophisticated methods −− but it still works," added Litan.
Source: http://www.techweb.com/wire/security/161600537

[Return to top]

Transportation and Border Security Sector

7. *April 27, Associated Press* — **Amtrak: Maker overestimated Acela brakes.** Amtrak President David Gunn said Wednesday, April 27, he believes the makers of the Acela Express trains overestimated the life expectancy of their brake rotors, forcing Amtrak to pull the entire fleet out of service for repairs. "I believe they misjudged the life of the rotors," Gunn told The Associated Press during a break in a House Appropriations subcommittee hearing on Amtrak's Fiscal 2006 budget. Bombardier and Alstom SA of France make the Acela trains, and have said the brakes were to last one million miles. The current Acela fleet had about half of that mileage, Gunn said. Gunn said the timetable for bringing back the Acela trains on a gradual basis was still this summer, adding that Bombardier and Alstom had yet to give Amtrak a delivery schedule for the brakes. Helene Gagnon, a spokesperson for Montreal−based Bombardier, Inc., said the companies hoped to have a schedule within a few days. Amtrak's chief operating officer Bill Crosbie said last week that the brake part is unique to the Acela and there was no active production line casting them. Crosbie said the companies had fewer than 70 disc brakes in stock. The Acela Express runs only along the Northeast corridor, with top speeds of 150 mph.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=513&ncid=718&e=8&u=/ap/20050427/ap_on_go_ot/amtrak_acela

8. *April 27, Associated Press* — **Man drives on taxiway at Iowa airport.** Air traffic at Des Moines International Airport was temporarily halted when a disoriented 70−year−old man drove in through an exit gate and led security on a chase onto an active taxiway. Duane Edwards Sheets drove through an open gate at the adjacent Iowa Air National Guard base on Tuesday, April 26, nearly striking a guard who tried to stop him, said Col. Greg Schwab, commander of the 132nd Air Fighter Wing. Airport security and police took over the chase after Sheets crossed onto airport property, where he drove along service roads, hit a fence and was chased onto an active taxiway, officials said. "They kept him off the main runway, but he was on the taxiway. That was probably the most dangerous part of it," Des Moines Police Capt. Richard Singleton said. Sheets faces state charges of criminal trespassing, aggravated assault and resisting officers. Federal authorities also planned to file charges, Singleton said.

Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−airport−chase,0,2290844.story?coll=sns−ap−nation−headlines

9. *April 27, Associated Press* — **Airbus A380 lands after making aviation history.** The world's largest passenger plane, the Airbus A380, completed its maiden flight Wednesday, April 27, a milestone for aviation and for the European aircraft−maker's battle with American rival Boeing Co. About 30,000 spectators watched the behemoth take off and touch down. The plane was carrying a crew of six and 22 tons of on−board test instruments. Airbus chief test pilot Jacques Rosay, flight captain Claude Lelaie and four crewmembers −− who all wore orange flight suits −− were taking no chances. Airbus had said they would be wearing parachutes during the first flight, in accordance with company policy. A handrail leads from the cockpit to an escape door that can be jettisoned if the pilots lose control of the plane. The A380, with a catalog price of $282 million, represents a huge bet by Airbus that international airlines will need bigger aircraft to transport passengers between ever−busier hub airports. But some analysts say signs of a boom in the market for smaller wide−body planes, such as Boeing's long−range 787 "Dreamliner," show that Airbus was wrong to focus so much time and money on its superjumbo.
Source: http://www.usatoday.com/travel/news/2005−04−27−airbus−flight_x.htm

10. *April 27, Associated Press* — **Arizona Minuteman border patrol may expand to Canadian border.** A controversial civilian patrol group that has been monitoring the Mexican border for illegal immigrants is planning to expand its mission to the Canadian border, organizers said Tuesday, April 26. Minuteman Project leaders said their volunteers, in one month, have alerted federal authorities to more than 330 cases of illegal immigrants crossing into the United States over a 23−mile stretch of Arizona's southern border. Now they plan to extend their patrol along the rest of the border with Mexico and are helping to organize similar efforts in four states that neighbor Canada. Chris Simcox, a Minuteman co−organizer who also operates Civil Homeland Defense, another Arizona group that monitors illegal immigrants, offered no timeline on when the Canadian border patrol −− to be organized in Idaho, Michigan, North Dakota and Vermont −− might begin. But he said he hoped to start patrols near San Diego, CA, by June and along the rest of the Mexico border by October. The U.S. northern border along Canada is twice as long as the southern border along Mexico. Customs officials caught a man with explosives trying to enter Washington State from Canada in December 1999 in what has become known as the millennium terrorist plot.
Source: http://www.usatoday.com/news/nation/2005−04−26−minutement_x. htm

11. *April 27, Inside Bay Area (CA)* — **Oakland port guarded by radiation detectors.** It took a little more than a year and almost $4 million, but California's Port of Oakland is now the most secure port in the nation when it comes to detecting radiation in shipping containers, U.S. Bureau of Customs and Border Protection officials said Tuesday, April 26. Unveiling one of its most prized achievements in the war against terrorism, the bureau showcased its radiation portal monitor, a tollbooth−like structure that detects radiation. And they chose Oakland for the unveiling because it is the first port in the nation to have every terminal "guarded" by the new technology. "All international container traffic that arrives in Oakland is now screened for nuclear materials or any source of radiation," said Nat Aycox, field director for the bureau's San Francisco office. "This program is part of our layer enforcement strategy to protect the country." At a cost of about $150,000 each, the 25 portals work like a metal detector at the

airport. Trucks drive through at a non−stop pace as the machine "reads" its cargo, searching for the dreaded "dirty bomb" or any item emitting radiation. By the end of the year, every port in California should have the portals in place at every terminal.
Source: http://www.insidebayarea.com/localnews/ci_2687774

12. *April 25, Transportation Security Administration* — **New technology for Access Control Enhancements.** The Transportation Security Administration (TSA) has announced the beginning of Phase II of the Airport Access Control Pilot Program in which TSA will test advanced technologies to enhance access control to secure areas of an airport. For example, working with Massachusetts Port Authority, TSA will take advantage of Logan International Airport's natural water boundary to test an advanced water perimeter intrusion detection system. The Port Authority of New York and New Jersey, along with TSA, will test a barrier−free boundary surrounding a cargo warehouse at John F. Kennedy. Working with Greater Orlando Aviation Authority, TSA will test equipment to monitor access of vehicles into secure areas of the airport at Orlando International Airport (MCO). Denver International Airport will test a barrier−free boundary surrounding a cargo warehouse at the airport using technology including ultrasonic emitters and microwave sensors. Salt Lake City Department of Airports will focus on enhancing access control to the baggage area entrance, which is part of the non−public, secure side of the airport. These technologies will be tested to determine both their effectiveness and impact on airport operations. TSA will collect and share data on the various technologies with the industry so they may utilize it for future projects.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 011d563

[Return to top]

Postal and Shipping Sector

13. *April 27, IDG News Service* — **Wireless technology secures vehicles.** The U.S. Postal Service uses wireless technology to manage industrial vehicles that sort the mail. New security applications can now monitor and lock down vehicles. In January, the Postal Service contracted with I.D. Systems Inc. and Unisys Corp. to develop an enterprise−wide wireless asset tracking system dubbed PIVMS, or Powered Industrial Vehicle Management System. The tracking technology will help the service manage industrial vehicles such as forklifts and secure 460 postal facilities nationwide. The system works when vehicles are wired with movement and impact sensors that are connected to a wireless transceiver inside the vehicle's cab. A keypad login on the hardware links to the vehicle's ignition system, and to a management server at each facility. To start a vehicle, an employee enters his identification number on the keypad. That information is then checked against an onboard database of authorized drivers. An unauthorized driver cannot start the vehicle. So in addition to tracking a vehicle's location, the technology can control vehicle access.
Source: http://www.computerworld.com/mobiletopics/mobile/story/0,108 01,101361,00.html

[Return to top]

Agriculture Sector

14. *April 27, New York State Department of Environmental Conservation* — **Chronic wasting disease found in New York wild deer.** The New York State Department of Environmental Conservation (DEC) Wednesday, April 27, announced it has received a preliminary positive result for chronic wasting disease (CWD) in a wild deer sampled in Oneida County. If confirmed, this will be the first known occurrence of CWD in the wild in New York State. The positive sample was from a yearling white−tailed deer, and was tested as part of DEC's intensive monitoring effort in Oneida County. The sample tissue was tested at the State's Veterinary Diagnostic Laboratory at Cornell University. The sample will be sent to the National Veterinary Services Laboratory in Ames, IA, to be verified. DEC implemented intensive monitoring efforts after CWD was found in two captive white−tailed deer herds in Oneida County –− the first incidents of CWD in New York State. To date, DEC, along with the U.S. Department of Agriculture's Wildlife Services program, has sampled 213 deer from Oneida County, and 25 deer from the Town of Arietta, Hamilton County. Since 2002, DEC has conducted statewide sampling of wild deer for CWD. When combined with sampling efforts in Oneida and Hamilton Counties, DEC has collected more than 3,700 samples from wild white−tailed deer.
    Source: http://www.dec.state.ny.us/website/press/pressrel/2005/20054 2.html

15. *April 27, Associated Press* — **Taiwan lifts ban on U.S. apples.** Taiwan on Wednesday, April 27, lifted a four−month ban on the import of U.S. apples, which was imposed after moth larvae had been found in several shipments, the Council of Agriculture said. The island introduced the ban in December 2004 after finding the codling moth larvae in a shipment from Oregon, but codling moths were detected in two previous shipments from Washington and California. Before the ban, more than half the apples on sale in Taiwan were imported from the U.S.
    Source: http://www.macon.com/mld/macon/business/11502141.htm

16. *April 27, Associated Press* — **Crop−threatening vine gains foothold in Indiana.** Kudzu, that notoriously fast−growing vine that covers vast tracts of the South, has spread to at least 28 Indiana counties, posing a threat to woodlands and the state’s soybean industry. Purdue University recently began studying some of the more than 70 patches of kudzu in the southern half of the state after stands of the invasive vine in Florida were found to harbor a deadly fungus that preys on soybeans. Soybean rust has not yet been found in Indiana, but plant pathologists believe it’s only a matter of time before the fungus shows up in the state. The fungus reached U.S. fields last fall, spreading as close to Indiana as Tennessee and Missouri. Kudzu’s early leafing vines would provide an early target for the fungus’ wind−borne spores to infect before spreading to soybeans later in the season, said Glenn Nice, a weed scientist with Purdue’s extension service. As part of his research, Nice is interested in whether Indiana kudzu is the same as the vines found in the South and how Indiana’s infestations got started. Purdue staffers will monitor some of the state’s kudzu stands for signs of the soybean rust fungus throughout the season.
    Source: http://www.fortwayne.com/mld/journalgazette/business/1150134 7.htm

[Return to top]

Food Sector

17.

April 26, Food Safety and Inspection Service — **Meat wrap recalled.** Prime Deli Corp., a Lewisville, TX, establishment, is voluntarily recalling approximately 191 pounds of meat wrap sandwiches that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday, April 26. The products were distributed to retail establishments in the Dallas− Fort Worth and Austin regions of Texas. The problem was discovered through routine FSIS regulatory sampling. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_022_2005_Relea se/index.asp

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

18. *April 27, United Press International* — **Ebola suspected in Equatorial Guinea.** The Minister of Health in Equatorial Guinea has issued an alert about the Ebola virus after a man with symptoms of the disease died last week. The minister advised any patient with symptoms of Ebola hemorrhagic fever, including a high fever and bleeding from the mouth, ears, nose or eyes, should be treated at a health facility. Ebola is one of the most deadly viral diseases known, killing 50 percent to 90 percent of those who become infected. It generally is spread by contact with bodily fluids of infected individuals, but the handling of infected chimpanzees also can transmit it. Neighboring country Gabon has had Ebola outbreaks several times in recent years.
Source: http://www.washingtontimes.com/upi−breaking/20050427−093159− 2340r.htm

19. *April 26, Scientist* — **NASA validated anthrax spore detection procedure in 1970s, but needs testing for biothreat agents.** Although federal administrators told Congress earlier this month that they didn't find all the anthrax that contaminated post offices in 2001 because no validated testing procedure existed at the time, Larry Kirschner, a NASA researcher who helped create a highly accurate procedure that the agency has used to test spacecraft for bacteria since the 1970s, said there's no reason it couldn't have been used to find anthrax in 2001. The NASA method involves streaking a wet swab made of cotton or soft plastic over a 25−square−centimeter surface. "The NASA standard assay technique is a well defined and reproducible technique for the recovery of [bacterial] spores from solid surfaces," Kirschner said. Linda Stetzenbach, of the University of Nevada, who testified before Congress earlier this month, told The Scientist that the NASA technique is now widely used outside the agency for other bacteria, over a standard area four times as large. Tanja Popovic, of the Centers for Disease Control and Prevention, testified at the hearing that no validated methods for sampling anthrax existed in 2001. She told The Scientist after the hearing that although the NASA technique is helpful, it cannot be considered validated for anthrax detection because "these

studies have not been done on biothreat agents," just bacterial spores in general.
Source: http://www.biomedcentral.com/news/20050426/02/

20. *April 26, Emerging Infectious Diseases* — **Highly pathogenic H5N1 influenza virus in smuggled Thai eagles.** On October 18, 2004, two Crested Hawk−Eagles (Spizaetus nipalensis) smuggled into Europe from Thailand were seized at Brussels International Airport in Belgiam. The eagles were transported in a hand luggage, with the zipper not totally closed to allow air to enter. The bird smuggler, a Thai resident, took connecting flights from Bangkok to Brussels, with a stopover in Austria; he placed his hand luggage in an overhead compartment during both flights. As import of birds and products from several Asian countries into the European Union (EU) is forbidden, the birds were destroyed and immediately sent to the Veterinary and Agrochemical Research Center for routine diagnosis to exclude influenza and Newcastle disease viruses. Samples were taken from lungs and injected into embryonating eggs, which died in two days. The isolated virus was denominated A/crested eagle/Belgium/01/2004. The antigenic subtyping as H5N1 was made by hemagglutination inhibition using 12 monospecific polysera. Passengers who had taken the same flights as the bird smuggler were informed by the media to seek medical advice if they had any influenza−like symptoms within seven days after the flight.
Source: http://www.cdc.gov/ncidod/EID/vol11no05/05−0211.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

21. *April 28, Associated Press* — **Emergency exercise to be held in Michigan this weekend.** Residents in Brighton, MI, are being told the large number of emergency personnel they will see on Saturday, April 27, are in town for an exercise. The 2005 Emergency Response Drill is part of a federally funded program to prepare the region in case of emergencies, such as terrorist attacks, Hazmat spills, hostage situations or explosions. The county's Emergency Management director says the simulation will involve first responders from Livingston and several surrounding counties. It will involve a scenario in which terrorists have exploded a dirty bomb during a concert. Another scenario will involve a hostage rescue from a middle school. Volunteers acting as real victims will play out situations during the drill.
Source: http://www.woodtv.com/Global/story.asp?S=3268519

22. *April 26, Linton Daily Citizen (IN)* — **Volunteers receive emergency response training.** Eleven two−person Community Emergency Response Teams (CERT) underwent 21 hours of intensive training in Switz City, IN, last weekend that will be provide invaluable assistance in the event of a natural disaster, like a tornado, earthquake, winter storm or a flood. Twenty−two volunteers completed the three−day certification course, the first sponsored by the Greene County Emergency Management Agency in cooperation with the State Emergency

Management Agency. CERT team members are trained to respond to disasters by turning off utilities when needed, suppressing small fires, treating life−threatening injuries with basic first aid, conducting light search and rescue operations, and helping victims cope with their emotions.
Source: http://www.dailycitizen.com/articles/2005/04/26/news/cert.tx t

[Return to top]

Information Technology and Telecommunications Sector

23. *April 27, US−CERT* — **Technical Cyber Security Alert TA05−117A: Oracle Products Contain Multiple Vulnerabilities.** Various Oracle products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include unauthenticated, remote code execution, information disclosure, and denial of service. Oracle released a Critical Patch Update in April that addresses more than seventy vulnerabilities in different Oracle products and components. The Critical Patch Update provides information about which components are affected, what access and authorization are required, and how data confidentiality, integrity, and availability may be impacted. US−CERT strongly recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate.
Critical Patch Update: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2 005.pdf
Source: http://www.us−cert.gov/cas/techalerts/TA05−117A.html

24. *April 26, Secunia* — **Sun Solaris multiple LibTIFF vulnerabilities.** Multiple vulnerabilities have been reported in LibTIFF, which potentially can be exploited by malicious people to compromise a user's system or cause a DoS (Denial of Service). A local user may be able to start a process that binds to a non−privileged network port to hijack future connections to the service that typically runs on that port.
Original advisory and updates:
http://sunsolve.sun.com/search/document.do?assetkey=1−26−577 69−1
Source: http://secunia.com/advisories/15113/

25. *April 26, FrSIRT* — **HP−UX Mozilla multiple vulnerabilities.** Multiple vulnerabilities were identified in HP−UX Mozilla, which may be exploited by malicious Websites to execute arbitrary commands. HP has acknowledged multiple vulnerabilities in Mozilla for HP−UX, which can be exploited by malicious people to cause a DoS (Denial of Service), gain knowledge of potentially sensitive information, bypass certain security restrictions, and compromise a user's system.
Upgrade to Mozilla HP−UX version 1.7.3.02: http://www.hp.com/go/mozilla
Source: http://www.frsirt.com/english/advisories/2005/0394

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: Multiple vulnerabilities were identified in MailEnable, which may be exploited by remote attackers to execute arbitrary commands. The flaw is due to a buffer overflow error in the HTTPMail Connector service.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 20525 (−−−), 135 (epmap), 1026 (−−−), 80 (www), 41170 (−−−), 2234 (directplay), 53 (domain), 1027 (icq), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

26. *April 27, TheDenverChannel* — **Box left during robbery forces bank evacuation.** Several streets in downtown Denver were closed for about 90 minutes Wednesday, April 27, morning after a bank robbery turned into an even more serious situation. Bomb squads were called to the Key Bank at 100 S. Broadway after a man walked inside at about 9:30 a.m., (11:30 a.m. ET), left a shoebox on the teller's counter and handed her a note saying that the box would blow up. The robber fled on foot with an unknown amount of cash but he left the box inside the bank. Because police did not know if the robber's threat was real, the bank was evacuated and a bomb squad was called in. The bomb squad went into the bank and used a type of water cannon to diffuse the device. A small shot was heard coming from inside the bank. Officers are still not sure if there was a real bomb inside the box.
Source: http://www.thedenverchannel.com/news/4421679/detail.html

27. *April 27, Bloomberg* — **New York City building guards to get counter−terrorism training.** New York City police have begun counter−terrorism classes for more than 50,000 private security guards in 4,000 of the city's largest office and apartment buildings, Police Commissioner Raymond Kelly said. Using intelligence gathered from terrorism incidents around the world, police trainers will teach the guards how to spot suspicious conduct and recognize false identification, Kelly said. The guards will be shown photos of explosive devices, learn how bombs have been placed in past attacks, and get pointers on how to spot a suicide bomber, he said. The announcement of the program comes a day after U.S. Homeland Security Secretary Michael Chertoff urged businesses in New York to voluntarily provide better security and coordination with government counter−terrorism efforts.
Source: http://www.bloomberg.com/apps/news?pid=10000103&sid=aOrhxeni zPxI&refer=us

[Return to top]

General Sector

Nothing to report.
[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:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.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 soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer