Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 20 May 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The U.S. Census Bureau has stopped an e−mail scam that lured individuals with a $5 instant cash reward to participate in a fake online "Operation Iraqi Freedom 2005 Survey." (See item 3)
- The Orange County Register reports a Cessna aircraft carrying six undocumented immigrants, including the pilot, took off from Fullerton Municipal Airport in California but was forced to land at Cannon Air Force Base in New Mexico, after running out of fuel. (See item 6)
- CNN reports top federal law enforcement officials say violent animal rights extremists and eco−terrorists now pose serious terrorism threats to the nation. (See item 25)

DHS/IAIP Update *Fast Jump*

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. *May 19, Associated Press* — **Michigan officials release annual energy outlook for summer.** Demand for electricity this summer is expected to nearly match the Michigan in−state production capability of utilities, forcing power companies to buy reserves, the state said Thursday, May 19, in its summer energy outlook. The Michigan Public Service Commission said total electric sales for 2005 are projected to increase about two percent over 2004 sales, due in part to a cooler−than−normal summer last year. "If we do have normal weather this

summer, the usage will go up due to increased use of air conditioners. That's really the main thing driving residential sales," said Jeff Pillon, the commission's manager for energy data security. With the summer's peak electricity demand for Detroit Edison Co. and Consumers Energy Co. expected at about 18,752 megawatts and the utilities capable of producing 19,207 megawatts, the companies have made plans to buy 15 percent and 11 percent reserve margins, the commission said. In hopes of preventing a blackout like the one in 2003, the commission has directed Michigan's electricity suppliers to report their supply levels. This year, "All of the reporting suppliers expect to have an adequate supply, including reserves, to meeting their anticipated loads," according to the commission's report.
Michigan Summer 2005 Energy Appraisal:
http://www.dleg.state.mi.us/mpsc/reports/energy/05summer/ea− summer05.pdf
Source: http://www.lansingstatejournal.com/apps/pbcs.dll/article?AID =/20050519/NEWS01/505190360/1001/RSS

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *May 20, Greenville News (SC)* — **Chemical spill triggers OSHA investigation.** The Occupational Safety and Health Administration (OSHA) will investigate an incident that occurred on Tuesday, May 17, at Southern Water Treatment in Greenville, SC where a large cloud of chemicals filled the air and injured 13 people, forcing the evacuation of nearby residents from their homes and businesses. Over the next few weeks, OSHA will look into whether there were workplace safety issues after an explosion caused the chemical spill, said Jim Knight, spokesperson for the agency. Greg Bowers, president of the company, said hydrogen sulfide was released into the air as chemicals were being mixed.
Source: http://greenvilleonline.com/news/2005/05/18/2005051864752.ht m

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *May 18, U.S. Census Bureau* — **Census Bureau stops phishing attack.** The U.S. Census Bureau on Wednesday, May 18, stopped an e−mail scam that lured individuals with a $5 instant cash reward to participate in a fake online “Operation Iraqi Freedom 2005 Survey.” The survey, however, was not a legitimate Census Bureau survey. The e−mail scam, which began at 7:49 a.m. EDT Wednesday, provided individuals with a link that took them to a fake Web page that appeared to be the official Census Bureau Internet site. After luring people into believing that they were at the actual Census Bureau home page, individuals were asked to answer five questions about their opinions on the Iraq War and provide their bankcard number and PIN to receive the $5 cash reward. The Census Bureau took immediate action and successfully shut

down the fake Web page at 12:20 p.m. EDT. The Census Bureau worked closely with the Department of Commerce and notified the appropriate law enforcement agencies about this fraudulent activity. The FBI is currently investigating to identify the individual(s) responsible for this deceptive and illegal financial scam.
Source: http://www.census.gov/Press−Release/www/releases/archives/miscellaneous/004873.html

4. *May 18, Netcraft* — **Online vigilantes fight back against phishers.** As scammers continue to target their victims with increasingly elaborate phishing sites, the surprise appearance of anti−phishing vigilantes is now hampering their operations. A PayPal phishing site recently reported was promptly taken down; not by the hoster or law enforcement agency, but seemingly by a vigilante with an interest in disabling such sites and protecting innocent Web users. The phishing site was replaced with a warning page, created with the open source OpenOffice.org suite on Windows. The identity of "sickophish" is not known, nor is it known how he gained access to the Web server to perform the act of vigilantism. Phishing sites are commonly found hosted on compromised Web servers, where lack of security allows scammers to access machines and upload phishing content. If a scammer exploits these security weaknesses without subsequently securing the machine, then online vigilantes are just as likely to exploit the weaknesses to go in and replace the fraudulent content.
Source: http://news.netcraft.com/archives/2005/05/18/online_vigilantes_fight_back_against_phishing_fraudsters.html

5. *May 18, Government Computer News* — **Industry executives ask for new notification law.** An industry group is asking Congress to pass a law requiring companies to notify consumers of security breaches, in part to stem the tide of state laws that threaten to create a patchwork of regulations. This is one of several recommendations made by the Business Software Alliance (BSA) at a forum it co−hosted Tues, May 17, with the Center for Strategic and International Studies to discuss its new report, Securing Cyberspace in the 21st Century. Recent high−profile incidents involving the loss or theft of personal data on thousands of people have triggered significant interest from Congress, the business community and the general public on taking steps to combat cybercrime, panelists at the forum agreed. However, the ability of law enforcement to keep up with these crimes is lagging, as criminals make use of computers and the Internet while government agencies struggle with outdated equipment and laws that never envisioned cybercrimes. BSA is proposing a federal law that would require companies to notify consumers if their personal information is lost or stolen.
Business Software Alliance: http://www.bsa.org
Center for Strategic and International Studies: http://www.csis.org/
Securing Cyberspace in the 21st Century: http://www.bsa.org/ceoinitiative/
Source: http://www.gcn.com/vol1_no1/daily−updates/35840−1.html

[Return to top]

Transportation and Border Security Sector

6. *May 19, Orange County Register (CA)* — **Illegal immigrants on flight.** A Cessna aircraft carrying six undocumented immigrants, including the pilot, took off from Fullerton Municipal Airport in California, earlier this week but was forced to land at Cannon Air Force Base in New

Mexico, after running out of fuel, authorities said Wednesday, May 18. The plane, which had crossed the country picking up undocumented Brazilian citizens in Boston and Fullerton while on its way to Atlanta, attracted little notice from airport or Homeland Security officials until its emergency landing Monday, May 16. It was the second time the pilot −− an illegal immigrant whose legally registered plane appears on Federal Aviation Administration records −− has flown undocumented immigrants, according to Immigration and Customs Enforcement (ICE) officials. The flight calls into question potential security vulnerabilities of Homeland Security agencies, as well as of small private and municipal airports, which often conduct little or no screening of small planes for undocumented immigrants, drugs and other illegal contraband, or for terrorist suspects. Smuggling of undocumented immigrants via small private aircraft is unusual because of the cost, ICE spokesperson Virginia Kice said. However, such methods may be more widespread than previously thought, especially at small airports, said Rod Propst, manager of Fullerton Municipal Airport.
Source: http://www.ocregister.com/ocr/2005/05/19/sections/local/loca l/article_526165.php

7. *May 19, Associated Press* — **Maine airport plays key role for no−fly diverted flights.** Officials are struggling to make sure the light is always on at the control tower at Bangor International Airport, which is playing a prominent role as a safe haven for planes diverted because of suspicious passengers. Twice in less than a week, Boston−bound international flights have been diverted to the airport because a passenger's name appeared on a no−fly list. Bangor is the first large U.S. airport for incoming European flights, and it's the last U.S. airport for outgoing flights, providing a safety net for aircraft with uncluttered skies and one of the longest runways on the East Coast. Officials who want Bangor to remain a beacon worry about a Federal Aviation Administration (FAA) proposal to scale back hours for the control tower. Maine Senator Susan Collins said the back−to−back diverted flights underscore the need to keep the control tower open 24 hours a day. The FAA proposal unveiled earlier this year would have the tower close between midnight and 5 a.m. FAA spokesperson Greg Martin said no final decisions have been made on the hours of operation of the control tower at Bangor and other airports.
Source: http://www.tuscaloosanews.com/apps/pbcs.dll/article?AID=/200 50519/APN/505190890&cachetime=3&template=dateline

8. *May 19, Associated Press* — **Ad campaign to warn illegal immigrants about desert crossings.** The Mexican Consulate in Tucson, AZ, will be running TV, radio and print ads warning would−be illegal immigrants about the dangers of crossing the border in Arizona. The ads, which will appear in Spanish−language media outlets throughout Arizona and the Mexican border state of Sonora, include testimonials from family members whose relatives have died, women who have been attacked and children who have been abandoned by smugglers. "We hope people will see these ads and decide not to cross, or convince their loved ones not to cross," said Juan Calderon, the Mexican consul in Tucson. Scores of illegal immigrants die each year while trying to cross Arizona's deserts during the summer, many of heat exposure. Migrants also fall prey to border bandits and smugglers who either abandon them in hostile terrain or hold them hostage while trying to extort more money from the crossers' family members.
Source: http://kvoa.com/Global/story.asp?S=3366684

9.

May 19, Department of Transportation — **Rail safety inspection capacity to triple.** The federal government will triple its capacity to inspect the nation's rail lines thanks to three new advanced track inspection vehicles being launched over the next year and a half, Department of Transportation Secretary Norman Y. Mineta announced on Wednesday, May 18. The announcement came during a visit to Baton Rouge, LA, where the Secretary got a demonstration of one of the new self−propelled inspection vehicles, the T−18, before it departs on its maiden voyage to identify track defects throughout Gulf Coast and Midwestern states. The Secretary noted that with the T−18 and two more inspection vehicles under construction, the Department of Transportation's Federal Railroad Administration would soon be able to inspect 100,000 miles of track each year, tripling the agency's current capacity. Mineta noted that the new inspection vehicles are a part of the National Rail Safety Action Plan, the Department of Transportation's aggressive new approach to improving safety throughout the railroad industry. The plan targets the most frequent, highest−risk causes of accidents, focuses federal oversight and inspection resources, and accelerates research into new technologies −− like the T−18 −− that can vastly improve rail safety.
National Rail Safety Plan: http://www.fra.dot.gov/downloads/Safety/action_plan_final_051605.pdf
Source: http://www.dot.gov/affairs/dot8105.htm

10. *May 19, Transport Topics* — **Southern California ports to install peak−hours fees.** Registration will begin next Monday, May 23, for a new program, known as OffPeak, aimed at reducing congestion at the ports of Los Angeles and Long Beach, CA, by setting fees for drivers operating in peak daytime hours, the group administering the program said Thursday, May 19. Beginning in the second half of July, all marine terminals at the ports will start OffPeak shifts on nights and weekends, with new fees added for cargo movement through the ports during peak daytime hours, with certain exceptions. Only registered users will be able to pay the fee. "OffPeak will play an important role in mitigating traffic congestion and air pollution around the ports, while helping the industry and community cope with growing cargo volumes," said Port of Long Beach Executive Director Richard Steinke.
Source: http://www.ttnews.com/members/topNews/0013093.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

11. *May 19, USAgNet* — **Soybean rust disease limited to Florida, Georgia so far.** Asian soybean rust continues to be of concern to soybean farmers in the United States, but the disease is presently restricted to Florida and Georgia. Seminole County, GA, is the latest county outside of Florida to report Asian soybean rust in 2005, according to the United States Department of Agriculture (USDA) Public Soybean Rust Website. The risk to northern soybean production regions during this season still remains largely unpredictable. If the disease is found widespread

in alternative hosts and volunteer soybeans in May in coast states, including Louisiana, Mississippi, and Alabama, computer models indicate that spores of the fungus can reach northern production regions before July. Early disease detection efforts will be conducted throughout many states during the 2005 growing season. Field locations at greater risk for disease will be monitored closely.
Source: http://www.usagnet.com/story−national.cfm?Id=519&yr=2005

12. *May 19, Washington Post* — **Two horses die from rare virus.** A disease believed to be equine herpes virus has swept through the barn area at Churchill Downs horse racing park in Louisville, KY, leading to the death of two horses and the placement of a quarantine on three barns. The outbreak of the rare neurological virus, which can cause symptoms ranging from mild fever and upper respiratory infection to paralysis, has led to the scratching of three horses scheduled to run this weekend in major stakes races at Pimlico race track in Baltimore, MD. Churchill Downs spokesperson John Asher said the facility is following the recommendation of the Kentucky Department of Agriculture regarding the quarantine, and there is no restriction on any horses not in the three restricted barns. An outbreak of the virus recently occurred in Maryland. Three horses were euthanized in March after contracting equine herpes virus at Columbia Horse Center in Columbia. Another horse died last month at the riding center, which currently is under quarantine.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/05/18/AR2005051801995.html

13. *May 19, Agence France Presse* — **Chinese officials find bird flu virus in eggs from Vietnam.** Checkpoint officials at China's Guangzhou international airport found 40 chicken, duck and goose eggs in passengers' luggage from two flights from Vietnam on April 28, Xinhua state news agency and Guangzhou Daily reported Thursday, May 19. Laboratory tests carried out by quarantine officials later found the eggs contained the H5N1 virus, the report said, citing Guangdong provincial quarantine authorities. The H5N1 strain of bird flu has been discovered in eight countries since late 2003, including China, Vietnam, Cambodia, Thailand, Indonesia, Japan, Laos and South Korea.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050519/hl_afp/healthchinavietnamflu_050519125508

[Return to top]

Food Sector

14. *May 18, Food and Drug Administration* — **Recalled brands of Tahini may still be on the market.** The Food and Drug Administration (FDA) is alerting the public that contaminated Ziyad brand Tahini and Ghandour Tahina Extra Sesame Butter may still be on the market despite a recall of these products in April 11, 2005. FDA is concerned that Ziyad Brothers Importing of Cicero, IL, which distributed both of these products, has not been as effective as possible in withdrawing the products from the market. FDA monitoring of the recall indicates that the company did not provide sufficient notice of the recall and all the products that are affected by it to all of its retail and other customers. FDA has issued a written notice of these findings to the company along with formal instructions on how the recall can be effectively completed. These products may be contaminated with Salmonella senftenberg, Salmonella

cubana, or Salmonella idikan, organisms which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems.
Original press release: http://www.fda.gov/oc/po/firmrecalls/ziyad04_05.html
Source: http://www.fda.gov/bbs/topics/ANSWERS/2005/ANS01358.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

15. *May 19, Reuters* — **Marburg fever contained, but death toll increases.** Marburg fever has killed more than 300 people in Angola, mainly through exposure to the deadly virus at home and at funerals, the World Health Organization (WHO) said on Thursday, May 19. The United Nations agency said Angolan health officials had reported 337 cases since late last year, 311 of them fatal. The vast majority of cases have been in the northern province of Uige, epicenter of the world's worst outbreak of the Ebola−like disease. "No cases have been reported outside Uige for the past five weeks," the WHO said in a statement. Despite better infection control at Uige hospital and collection of unsafe syringes in homes, new cases "continue to be linked to exposure in homes and at funerals, indicating that public understanding of the disease still needs to be improved," it said. Experts say many cases have been contracted by people caring for loved ones in the final stages of illness or through washing and kissing bodies after death in accordance with local custom.
Source: http://www.reuters.com/newsArticle.jhtml?type=worldNews&storyID=8541417&src=rss/worldNews

16. *May 18, CBC News (Canada)* — **Fourth case of hantavirus in Canada.** Health authorities in Alberta, Canada, are looking for help from Health Canada to deal with a small outbreak of the hantavirus, a potentially fatal disease. Officials have confirmed a fourth case after one woman died last week and another adult and child from the same family in central Alberta became ill. They say a man from Hobbema, south of Edmonton, has come down with the infection. Dr. Karen Grimsrud, deputy provincial health officer, says the latest case is not related to the first, but that makes it a bigger concern. "I think it leaves us with a question that we had last week and that is, there's something unusual going on here, how can we explain this cluster?" said Grimsrud. Grimsrud says the province has asked for Health Canada's assistance to determine whether there is a higher percentage of mice infected in the area. Hantavirus is a respiratory illness spread by infected deer mice through their droppings, their urine or their saliva. It's most common in the spring, when people are outdoors or doing spring cleaning and breathing in air−borne particles.
Source: http://www.cbc.ca/story/canada/national/2005/05/18/Hantaviru sAB_050518.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

17. *May 19, Journal Gazette/Times−Courier Online (IL)* — **Mock fire disaster leaves college district dead in cyberspace.** A mock fire disaster drill at Lake Land College in Mattoon, IL, Wednesday, May 18, produced more than make−believe damage and death. The mock fire also left the college district dead in cyberspace by striking in the college data center operated by Information Systems and Services. The surprise drill was conducted shortly after 7 a.m. Wednesday, to test the response of employees with Public Safety, Maintenance, Information Systems and Services and Public Relations as well as Mattoon Fire Department. The drill produced a situation where a fire had destroyed or damaged computer server racks and seriously injured an employee in the data center. "Every year I do something like this with my personnel," said Lake Land Public Safety Captain Randy Irvin as he inspected the building about an hour after the fire was reported. The scenario not only required the college to tend to the death of an employee and secure a fire−damaged building, but also attempt to rebuild computer servers affecting people across the college district and even the country when on−line classes are considered. The fire was geared to be happening when classes were in session, not between the spring and summer semesters.
Source: http://www.jg−tc.com/articles/2005/05/19/news/news003.txt

18. *May 19, USA TODAY* — **FEMA chief defends agency's response to Florida storm.** The head of the government's disaster−relief agency on Wednesday, May 18, disputed an audit that found the agency wasted millions of dollars after Hurricane Frances last fall. Federal Emergency Management Agency (FEMA) chief Michael Brown said he was proud of the agency's response to an "unusually cruel" storm season. The audit by the Department of Homeland Security's inspector general charged that lax inspection policies left FEMA open to "fraud, waste and abuse" and that FEMA doled out $31 million to Miami−Dade county residents who may not have deserved any money. In some cases, payments went to people who had no property damage. Brown urged senators investigating FEMA's hurricane response to remember that in fall 2004, Florida was hit with four hurricanes in six weeks −− an unprecedented disaster. Given the magnitude of the damage, Brown said he had to quickly hire and train thousands of new inspectors.
Source: http://www.usatoday.com/news/washington/2005−05−18−fema−chie f_x.htm

19. *May 19, Reuters* — **FCC tells Internet phone carriers to provide 911 service.** U.S. regulators on Thursday, May 19, ordered Internet telephone carriers to provide full 911 emergency calling services to customers later this year, after hearing from people who were unable to get through during life−threatening crises. The Federal Communications Commission (FCC) voted unanimously to require carriers to ensure that 911 calls from Internet phones will reach live emergency dispatchers instead of being connected to administrative lines. In addition, the carriers will have to provide callers' numbers and addresses. In most cases, calls to 911 with

traditional phones go to live dispatchers who have the address and number of the caller pop up on their computer screen. But that does not always happen with Voice over Internet Protocol (VOIP) calls, which start out over high−speed Internet connections. Under the new rules, carriers like Vonage Holdings Corp., the biggest VOIP provider, would have to provide the 911 services to customers regardless of whether they use it in a single location or multiple places. There are more than one million VOIP customers in the United States already. Telephone and cable carriers are rolling it out because it is cheaper for both subscribers and the companies.
Source: http://www.reuters.com/newsArticle.jhtml?type=internetNews&s toryID=8546689

20. *May 19, Department of Homeland Security* — **Commercial Equipment Direct Assistance Program awards announced.** The Department of Homeland Security on Thursday, May 19, announced the first round of awards under the new Commercial Equipment Direct Assistance Program (CEDAP). The awards provide equipment for communications interoperability, information sharing, chemical detection, sensor devices, and personal protective equipment to 214 jurisdictions throughout the nation. Equipment awarded totals $2,044,680. The FY 2005 Appropriations Act directed DHS to assist selected smaller jurisdictions by providing antiterrorism equipment and technology. Awards are being made to law enforcement and emergency responder agencies not currently funded through the Urban Area Security Initiative (UASI). “CEDAP provides equipment and training to jurisdictions across the country as part of a unified effort− from urban to rural areas—to build sustainable capabilities in the fight against terrorism,” said Matt A. Mayer, Acting Executive Director of the Office for State and Local Government Coordination and Preparedness. National law enforcement associations including the International Association of Chiefs of Police and the National Sheriffs’ Association have heralded CEDAP for providing equipment directly to jurisdictions.
Commercial Equipment Direct Assistance Program Award Recipients list:
http://www.dhs.gov/dhspublic/interweb/assetlibrary/Press_CED APAwards_05−19−05.pdf
Source: http://www.dhs.gov/dhspublic/display?content=4504

[Return to top]

Information Technology and Telecommunications Sector

21. *May 19, Zone−H.org* — **ZENworks Remote Management fails to properly validate authentication.** This authentication protocol contains several stack and heap overflows that can be triggered by an unauthenticated remote attacker to obtain control of the system that requires authentication. Successful exploitation of ZENworks allows attackers unauthorized control of related data and privileges on the machine and network. It also provides attackers leverage for further network compromise. There is no solution at this time.
Source: http://www.zone−h.org/en/advisories/read/id=7524/

22. *May 19, Networking Pipeline* — **Interest in IPv6 found to be lagging.** Although it has been in the works for a decade, the next−generation Internet protocol IPv6 has failed to excite the interest of key decision makers in the federal government and private sector, according to a survey by equipment vendor Juniper Networks. Juniper's Federal IPv6 IQ Study found that less than 7% of respondents consider IPv6 "very important to achieving their IT goals," despite the fact that the protocol is designed to address, among other things, many of the quality of service, security, and network management issues that concern them. The Federal government is

particularly indifferent to IPv6 and lags well behind the private sector in migration planning and awareness. Published by the Internet Engineering Task Force in RFC2460 in 1995, IPv6 provides a larger IP address space and provides native support for packet encryption, header authentication, IPsec virtual private networking, multicasting and dynamic address configuration.
Study: http://www.juniper.net/federal/IPv6/
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=163105617

23. *May 17, SecuriTeam* — **Linux Kernel pktcdvd and rawdevice ioctl race condition.** Two locally exploitable flaws have been found in the Linux rawdevice and pktcdvd block device ioctl handler that allows local users to gain root privileges and also execute arbitrary code at kernel privilege level. The Linux kernel contains pktcdvd and rawdevice block device components. Due to the missing checks in pktcdvd and rawdevice ioctl handler parameter, the process can break user space limit and execute arbitrary code at kernel privilege level. There is no solution at this time.
Source: http://www.securiteam.com/unixfocus/5GP0F20FQI.html

24. *May 16, SecuriTeam* — **Neteyes Nexusway's multiple vulnerabilities.** There are multiple vulnerabilities in Neteyes Nexusway which could permit a malicious attacker to gain full control over the product. By sending crafted HTTP cookies, any user with access to port 443 on Neteyes Nexusway may use these vulnerabilities to become Neteyes Nexusway administrator. This will allow user to change any configuration on this device. There is no solution at this time.
Source: http://www.securiteam.com/securitynews/5CP0B20FQM.html

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: US−CERT has received numerous reports of spam messages containing German and/or English text. It is believed that the spam messages are generated by a variant of the Sober worm family. The spam arrives with politically−themed messages in German and contains links to news articles on German Web sites.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 1026 (−−−), 27015 (halflife), 135 (epmap), 6881 (bittorrent), 53 (domain), 1025 (−−−), 1433 (ms−sql−s), 139 (netbios−ssn), 80 (www) 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

Nothing to report.
[Return to top]

General Sector

25. *May 19, CNN* — **FBI, ATF address domestic terrorism.** Violent animal rights extremists and eco−terrorists now pose one of the most serious terrorism threats to the nation, top federal law enforcement officials say. Senior officials from the FBI and the Bureau of Alcohol, Tobacco, Firearms (ATF) and Explosives told a Senate panel Wednesday, May 18, of their growing concern over these groups. Of particular concern are the Animal Liberation Front and the Earth Liberation Front. John Lewis, the FBI's deputy assistant director for counterterrorism, said animal and environmental rights extremists have claimed credit for more than 1,200 criminal incidents since 1990. In the same period violence from groups like the Ku Klux Klan and anti−abortion extremists have declined, Lewis said. ATF Deputy Assistant Director Carson Carroll said, "The most worrisome trend to law enforcement and private industry alike has been the increase in willingness by these movements to resort to the use of incendiary and explosive devices." The FBI also identified a British−based group, Stop Huntingdon Animal Cruelty, as a U.S. terror threat. The group targets Britain's Huntingdon Life Sciences Laboratory, which has an American facility in East Millstone, NJ.
    Source: http://www.cnn.com/2005/US/05/19/domestic.terrorism/index.ht ml

[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) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 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