Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 19 May 2005

Current Nationwide Threat Level is

For info click here
http://www.dhs.gov/

Daily Highlights

- The New York Times reports graduate students in a computer security course worked on a project finding personal information on the Internet, and proved that all it takes to obtain reams of personal data is Internet access, a few dollars, and some spare time. (See item 4)
- WBOC TV16 reports all nine counties on Maryland's Eastern Shore will soon be connected through a new emergency planning system to allow them to communicate and respond to large−scale emergencies, like terrorist attacks and natural disasters. (See item 19)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact 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. *May 19, Associated Press* — **Nuclear plant security officers spot possible break−in.** Security officers on perimeter patrol at the Oconee Nuclear Station, located near Greenville, SC, apparently spotted an attempted break−in at a maintenance and warehouse facility across from the nuclear plant, officials said. Two people were trying to get through a fence, spokesperson Dayle Stewart said. They realized they had been seen and fled, Stewart said. Duke Power, which operates the nuclear station, parks utility trucks and has an equipment warehouse within the fence at an operations center. But the area is completely unrelated to the nuclear operation, Stewart said. Wire and other equipment is also stored there, she said.
Source: http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/ local/11670224.htm

2. *May 18, Associated Press* — **Double derailment disrupts coal traffic.** Two separate train derailments that occurred last weekend in Converse County, WY, disrupted coal train traffic in northeast area of the state. "Between those two derailments, we've had quite a service disruption in that area," John Bromley, spokesperson for Union Pacific railroad, said Tuesday, May 17. As many as 100 trains a day ship coal from mines in northeast Wyoming's Powder River Basin. The cause of the derailments is under investigation, but weather and track conditions are considered potential causes.
Source: http://www.casperstartribune.net/news/wyoming/4bf0b1635a3fec7787257005005897cf.txt

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *May 18, The Register (UK)* — **Home computers launch phishing attacks.** Phishing attacks are growing more sophisticated as attackers devise ever more devious means to stay at least one step ahead of banks and others fighting the contain fraudulent scams, according to a study from the Honeynet Project. The report, Know your Enemy: Phishing, draws on data collected by the German Honeynet Project and UK Honeynet Project and focuses on picking apart real world incidents to discern the tactics of phishing fraudsters. As with a previous study on botnets, the findings come from monitoring a network of personal computers deliberately left open to attack. What emerged from the study is the most detailed technical description of the operating method of phishing attacks seen to date. It also discovered that lax security practices by consumers and small business are giving scammers a base from which to launch attacks. The researchers discovered that phishers compromised honeypot machines for four main purposes: to set up phishing Websites targeting well−known online brands; sending junk mail e−mails advertising phishing Websites; installing redirection services to deliver Web traffic to existing phishing Websites or for the propagation of spam and phishing messages via botnets.
Report: http://www.honeynet.org/papers/phishing/
Source: http://www.theregister.co.uk/2005/05/18/honeynet_phishing_research/

4. *May 18, New York Times* — **Students find personal data easily available.** A class of 41 graduate students in a computer security course at Johns Hopkins University in Baltimore, MD, worked on a project finding personal information on the Internet, and proved what privacy advocates have been saying for years −− all it takes to obtain reams of personal data is Internet

access, a few dollars and some spare time. Working with a strict requirement to use only legal, public sources of information, groups of three to four students set out to vacuum up not just tidbits on citizens of Baltimore, but whole databases: death records, property tax information, campaign donations, and occupational license registries. They then cleaned and linked the databases they had collected, making it possible to enter a single name and generate multiple layers of information on individuals. Each group could spend no more than $50. Several groups managed to gather well over a million records, with hundreds of thousands of individuals represented in each database.
Source: http://www.nytimes.com/2005/05/18/technology/18data.html

5. *May 17, Savannah Morning News (GA)* — **University hacker puts bookstore customers at risk.** The FBI and state investigators in Georgia are trying to figure out how tens of thousands of Georgia Southern University (GSU) bookstore customers fell prey to a computer hacker. Although no incidents of theft or fraud have been reported, university officials are warning students, alumni and bookstore customers that Social Security numbers and credit card information were put at risk on April 23, when someone hacked into the bookstore's computer system, said GSU spokesperson Rosemary Carter. The server contained names, credit card numbers and expiration dates of those who made credit card purchases. It also included Social Security numbers of those who used checks, according to Carter. Until recently, Georgia drivers' licenses contained drivers' Social Security numbers. Campus officials said they are unsure the extent of the security breach, but said tens of thousands people are at risk.
Source: http://savannahnow.com/stories/051705/3037421.shtml

6. *May 17, IDG News Service* — **Secret Service director calls for cybersecurity cooperation.** Companies with compromised data have a duty to report that information to investigators as a way to keep others from being victimized, said Ralph Basham, the director of the U.S. Secret Service, on Tuesday, May 17. The Secret Service, which has jurisdiction to investigate financial crimes, is working hard to prevent Internet−related crimes such as identity theft, but it needs assistance from private companies, said Basham, speaking at an event on organized cybercrime in Washington, DC. Compromises that affect one company are increasingly rare in a world connected by the Internet, Basham added. Still, the sharing of information between law enforcement agencies and private industry remains an area that needs significant improvement, said a group of IT security experts, speaking on a panel discussion following Basham's remarks. Technology that could help reduce cybercrime does exist, but law enforcement agencies conducting investigations often don't immediately share information about new threats, said Albert Sisto, CEO of Phoenix Technologies, a security software vendor. Federal law enforcement agencies are trying to share more information, but it's often difficult to disclose too much information without compromising an active investigation, responded Kimberly Peretti, a lawyer in the Computer Crime and Intellectual Property Division at the Department of Justice.
Source: http://www.networkworld.com/news/2005/051705−secret−security .html

[Return to top]

Transportation and Border Security Sector

7. *May 18, Associated Press* — **Senate passes highway bill; veto possible.** The Republican−controlled Senate passed a $295−billion highway bill, saying massive spending on

bigger and better roads is necessary to fight congestion and unsafe roads. The Bush administration, while pressing Congress to pass a new bill, said the Senate version was too expensive in a time of war and debt and could result in the first veto of the Bush presidency. In March, the House passed a $284−billion bill, the maximum the White House says it will accept without a veto. The Senate now must work out differences with the House−passed bill, which in addition to approving less money specifies thousands of projects requested by lawmakers, from bike paths to sidewalks. Almost all of the Senate money is divided among the states by a complicated formula. In addition to granting money to states to repair and build roads and bridges, the bill would provide more than $50 billion nationally to fund public transit and recreational road programs and to promote highway safety.
Source: http://www.freep.com/news/nw/roads18e_20050518.htm

8. *May 18, Department of Transportation* — **Amtrak's losses underscore need for reform.** Last year, Amtrak lost more than $908 million on its 15 long distance routes, yet there is little evidence to believe that the company will do anything to reverse the massive losses in taxpayer funds unless reforms are passed by Congress this year, Department of Transportation Secretary Norman Y. Mineta said Wednesday, May 18, during a visit to Amtrak's station along the Sunset Limited line in Mobile, AL. Mineta made the appearance in Alabama as part of National Transportation Week to call for reform of Amtrak. This visit is part of his push for legislation to save inter−city passenger rail through federal financial support, a partnership with the states, more local control of service and schedules, and competition among operators. Mineta stressed that long distance trains could and should continue to play an important role in the nation's transportation system. He cited the Alaska Railroad as an example of a company that has developed a successful approach to long distance trains. The Alaska Railroad is profitable because it has found a way to meet the needs of local travelers while bringing cruise ship passengers inland, Mineta noted.
Source: http://www.dot.gov/affairs/dot7605.htm

9. *May 18, Transport Topics* — **AAA projects record Memorial Day travel.** A record 37.2 million Americans will travel over the Memorial Day holiday weekend despite the highest gasoline prices ever recorded for a holiday, AAA said Wednesday, May 18. The number of Americans who will travel 50 miles or more from home this holiday is a 2.2% increase from last year, the travel association said. About 31 million travelers, or 84%, expect to travel by motor vehicle, a 2.2% increase from the 30.5 million who drove a year ago, AAA said. Another 4.2 million, or 11%, plan to travel by airplane, 3.2% higher than last Memorial Day. Another 1.9 million vacationers, or 5%, will travel by train, bus, or other mode, about the same as a year ago, the group said. "Prices might be 15 cents per gallon higher than last year's then−record levels, but gasoline remains a relatively small part of most travelers' vacation costs. Look for another crowded holiday on the highways," said Sandra Hughes, AAA Travel's vice president. Holiday auto travelers will find gas prices nationwide currently averaging about $2.15 for a gallon of regular gasoline −− a drop of nine cents over the past month, but about 15 cents higher than the last year.
Source: http://www.ttnews.com/members/topNews/0013089.html

10. *May 17, Department of Transportation* — **Hurricane recovery funds for Florida's roads and bridges.** Florida received almost $1 billion in federal hurricane recovery funding on Tuesday, May 17, to help the region get back on its feet in the wake of last year's onslaught of

devastating storms. Department of Transportation Secretary Norman Y. Mineta made the announcement at a news conference with Governor Jeb Bush at the Florida capitol. Mineta said Florida will receive $928 million through the Federal Highway Administration's Emergency Relief program to reimburse the state for past and future damage repair work to help restore Florida's highways and bridges to their pre−hurricane condition. The Secretary said the funding will be used to cover the state's costs to rebuild washed out highways, and repair or replace damaged bridges that serve as a vital lifeline to Florida residents. The emergency relief program provides funding for the repair or reconstruction of federal−aid highways and roads on federal lands which have suffered serious damage as a result of natural disasters. Hurricane recovery funds also were awarded to nine other states including Alabama, Delaware, Georgia, North Carolina, Ohio, Pennsylvania, South Carolina, Virginia and West Virginia. Puerto Rico also received recovery money.
Emergency Relief FUNDS CHART: http://www.dot.gov/affairs/ERfunds.htm.
Source: http://www.dot.gov/affairs/dot7905.htm

11. *May 17, CNN* — **New air cargo rules proposed.** With hope of closing a loophole in airline security nearly four years after the attacks of September 11, 2001, lawmakers Tuesday, May 17, introduced two amendments to the 2006 Department of Homeland Security authorization bill. The first would mandate the inspection of all cargo before it is shipped on passenger airplanes by 2008. Until that date, the second amendment would require airlines to notify passengers when unscreened cargo is being shipped in the cargo hold of a passenger plane. "Twenty−two percent of all the air cargo that is transported in the United States is loaded aboard passenger planes," said Rep. Ed Markey, (D−MA), a co−author of the bipartisan legislation. The Transportation Security Administration (TSA) relies now on what's called the "known shipper" database, a list of outfits approved by TSA to ship with little or no screening. "The agency inspects at−risk cargo that presents the greatest security threat, using current explosives detection technologies, canine teams or visual inspection," said TSA spokesperson Amy von Walter.
Source: http://www.cnn.com/2005/TRAVEL/05/17/air.cargo.security/inde x.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

12. *May 17, U.S. Department of Agriculture* — **USDA official announces roundtable discussion.** The U.S. Department of Agriculture (USDA) will hold a roundtable discussion on June 9 regarding the safety of North American beef and the changing infrastructure of the industry. Secretary Mike Johanns, who made the announcement on Wednesday, May 17, noted that data illustrating the success of USDA's enhanced BSE surveillance program will be part of the roundtable discussion entitled "The Safety of North American Beef and the Economic Effect of BSE on the U.S. Beef Industry." The enhanced surveillance program targets the population of

animals in which BSE is most likely to be detected, including non−ambulatory or downer animals, animals exhibiting signs of a central nervous system disorder or any other signs that could be consistent with BSE and animals that die from unknown causes. More than 350,000 animals have been tested and all have been negative. The event will bring together USDA experts, producers, packers, other industry groups and academia to discuss the science of BSE and the economic impacts on the U.S. beef industry.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2005/05/0168.xml

13. *May 17, North Dakota Department of Agriculture* — **West Nile virus detected in North Dakota horse.** One case of West Nile Virus (WNV) was confirmed in Burleigh County, North Dakota last week, the first in two years. Dr. Susan Keller, the state veterinarian, said horse owners who have not had their horses immunized or who have not yet arranged to have booster shots for their animals, should contact their veterinary practitioner. “It takes several weeks for the immunizations to take full effect, so the sooner any non−immunized horse is vaccinated, the better chance it has of resisting the disease,” Keller said. WNV was first detected in the western Hemisphere in 1999. In 2002, more than 15,250 equine cases were reported in the U.S., most notably in the central portion of the country from Texas to Minnesota. In 2003, 5,181 equine cases were reported, and in 2004 only 1,341 equines cases of WNV were reported, less than 10 percent of the 2002 totals. WNV is spread by mosquitoes that feed on infected birds and subsequently pass it to other animals. The virus causes a form of encephalitis or inflammation of the brain. It affects humans, horses, birds and, less commonly, other animals.
Source: http://www.agdepartment.com/2005Press/other050517.htm

[Return to top]

Food Sector

14. *May 17, Food and Drug Administration* — **CaJohns Fiery Foods recalls barbeque sauces.** CaJohns Fiery Foods Company is voluntarily recalling 16−ounce glass bottles and one−gallon size plastic jugs of several brands of barbeque sauces because they contain undeclared anchovies, soybeans, and wheat. People who have allergies to these ingredients run the risk of serious or life−threatening allergic reaction if they consume these products. The specific brands of barbeque sauces being recalled are CaBoom! Bayou−Q Barbeque Sauce Spicy, CaBoom! Barbeque Sauce Hot, CaBoom! Bayou−Q Barbeque Sauce X Hot, Gecko Gary’s Brushfire Spicy BBQ Sauce, Irish Scream BBQ Sauce, and HDH Grillin’ Sauce. All lot codes of these sauces are being recalled for re−labeling. The recalled barbeque sauces were distributed nationwide through retailers, mail order and Websites. The firm has suspended distribution of these products until a new revised label listing the undeclared ingredients is acquired. No illnesses have been reported to date in connection with this problem.
Source: http://www.fda.gov/oc/po/firmrecalls/cajohns05_05.html

15. *May 12, University of Minnesota Extension Service* — **Protecting food system from intentional attack is topic of four workshops.** Four regional workshops will be hosted by the University of Minnesota Extension Service in June and July entitled, "Protecting Our Food System from Intentional Attack." The seminars are funded by the University of Minnesota's Center for Public Health Preparedness and the Center for Public Health Education and Outreach

through a grant provided by the Centers for Disease Control. The workshops are targeted toward people working in Minnesota's food industry. Participants will learn about the intentional and unintentional threats that could affect agriculture and our closely related food industries. The workshops will focus on building relationships and planning to prevent and respond to food system emergencies, including the threat of terrorism. A highlight of the session will be a "tabletop exercise" that will focus on an outbreak of avian influenza, a disease that has significant animal health, human health, and food safety implications, including the possibility of a pandemic disease outbreak. Participants will work closely with other community members, emergency response professionals and governmental representatives charged with agricultural/food emergency response preparedness.
Source: http://www.extension.umn.edu/extensionnews/2005/protectingfo od.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

16. *May 18, IRIN News* — **Polio cases increase in Yemen.** The number of confirmed polio cases in Yemen has risen again this week to 83 with another 411 suspected, according to aid agencies. The World Health Organization (WHO) and United Nations Children's Fund (UNICEF) announced the increase at a press conference in the capital, Sana on Tuesday, May 17. "The number of confirmed polio cases has reached 83 across six provinces. This number could increase to 200, as many more suspected cases are still being investigated," said WHO representative for Yemen, Dr. Hashim Al−Zain. The most badly affected governorates are Hodeidah in the west, Sana and Taiz in the south, along with Hadramawt in the east and Amran in the north. Yemen was designated polio free by WHO in 1996 and officials say the latest outbreak was brought in from Africa. Polio is a highly infectious viral disease which invades the nervous system and can cause total paralysis in a matter of hours.
Source: http://www.irinnews.org/report.asp?ReportID=47160&SelectRegi on=Middle_East&SelectCountry=YEMEN

17. *May 18, Reuters* — **WHO confirms Ebola outbreak in Congo.** Ebola has returned to the Republic of Congo, killing nine people since the end of April, the World Health Organization (WHO) said on Wednesday, May 18, after tests confirmed the presence of the deadly virus. "The results (of laboratory tests) came in yesterday ... It is indeed a case of Ebola," said Adamou Yada, WHO's representative in Congo, which has faced serious outbreaks of the disease in the past. The latest outbreak is in the forested northwestern Cuvette−Ouest region, where nearly 150 people died from Ebola in 2003. "Since the beginning (of the outbreak), we have registered 11 cases, including nine deaths," Yada said. There is no known cure for Ebola, which is passed on by infected body fluids and kills between 50 and 90 percent of victims, depending on the strain. In a statement on its Website, WHO said of the 11 cases in Congo, one had been confirmed as Ebola by laboratory tests and 10 were epidemiologically linked. A total

of 81 contacts were being monitored in the towns of Etoumbi and Mbomo, it said. Scientists think past outbreaks in Cuvette−Ouest, near the border with Gabon, were caused by the consumption of infected monkey meat.
WHO Statement: http://www.who.int/csr/don/2005_05_18/en/index.html
Source: http://www.reuters.co.uk/newsArticle.jhtml?type=worldNews&storyID=730401&section=news&src=rss/uk/worldNews

18. *May 17, Bloomberg* — **Vietnam bird−flu pattern suggests virus is evolving, WHO says.** The pattern of human bird flu infections in Vietnam, the nation hit hardest by the disease, suggests the H5N1 virus that causes the illness is evolving in ways that make it more contagious, according to a report from the World Health Organization (WHO). Changes in bird−flu, or avian influenza, cases in northern Vietnam include detection of asymptomatic infections, a wider age range of people infected and fewer deaths from the disease, the WHO said in a recent report titled "WHO Inter−country Consultation Influenza A/H5N1 in Humans in Asia." It is "possible" that the changes show that H5N1 viruses are becoming more capable of human−to−human transmission, the agency said. "The viruses are continuing to evolve and pose a continuing and potentially growing pandemic threat," the WHO said. "It is possible that the avian H5N1 viruses are becoming more infectious for people, facilitating infection in a greater number or range of people and resulting in more clusters." Some epidemiological features of bird flu cases in northern Vietnam during the country's outbreak since the end of last year appear to differ from cases reported earlier and in southern Vietnam during the same time period, the WHO said in the review. The WHO report said it was unlikely the new epidemiological patterns were random variation.
WHO Inter−country Consultation Influenza A/H5N1 in Humans in Asia: http://www.who.int/csr/disease/avian_influenza/H5N1%20Intercountry%20Assessment%20final.pdf
World Health Assembly: Strengthening pandemic influenza preparedness and response, Report by the Secretariate: http://www.who.int/gb/ebwha/pdf_files/WHA58/A58_13−en.pdf
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=aaNUsm2n8Iks&refer=asia

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

19. *May 18, WBOC TV16 (MD)* — **Emergency planning system for Maryland's Eastern Shore.** For the first time ever, all nine counties on Maryland's Eastern Shore will be connected through a new emergency planning system. On Monday, May 16, Governor Robert Ehrlich unveiled the plan during a live statewide Web cast, along with the mayors from Ocean City and Cambridge. The plan will allow the counties to better communicate and respond to large−scale emergencies, like terrorist attacks and natural disasters. Ocean City Mayor Jim Mathias said,

"This really gives us a better opportunity for all our counties on the Eastern Shore to talk together, work together, make notifications together and be connected back to the command center."
Source: http://www.wboc.com/Global/story.asp?S=3360644&nav=MXEFa0Gh

20. *May 18, Associated Press* — **FEMA gave $31M in aid to the unqualified.** The Federal Emergency Management Agency (FEMA) gave more than $31 million to thousands of Floridians who may not have qualified for any disaster aid after Hurricane Frances, one of several findings of a federal audit that said the aid system was vulnerable to fraud. The finding, released to a Senate committee Wednesday, May 18, said FEMA granted requests for aid in Miami−Dade County on verbal assurances, without proof of damage like repair receipts or proof of ownership. "It was a pay first, ask questions later approach," said Sen. Susan Collins (R−ME), chair of the Homeland Security and Governmental Affairs Committee. The report came from the Department of Homeland Security's Office of Inspector General, which said the questionable payments were the latest in a string of evidence that the agency's payout system is vulnerable to widespread waste, fraud and abuse. Inspectors recommended that FEMA take a range of steps to tighten assessment standards and safeguards against abuse. FEMA chief Michael D. Brown said he regretted the findings, but said such problems are not widespread in his agency.
Source: http://www.boston.com/news/nation/washington/articles/2005/05/18/fema_gave_31m_in_aid_to_the_unqualified/

21. *May 17, Southern Maryland Online* — **Funds for fire grant programs.** Congressman Steny Hoyer (D−MD), Co−Chair of the Congressional Fire Services Caucus, on Tuesday, May 17, successfully added an amendment to the 2006 Homeland Security Appropriations bill to provide an additional $50 million in funding to firefighter grant programs −− $25 million for the Assistance to Firefighter Grant Program and $25 million for the Staffing for Adequate Fire and Emergency Response (SAFER) Firefighter Grant Program. The Fire Grant Program was established by Congress in 2000 to meet the basic equipment, training and firefighter safety requirements of America's fire service, and to bring all fire departments to a baseline of readiness to respond to all hazards. The Fire Grant program has been a tremendous success, providing more than $3 billion nationally, and more than $24 million in Maryland, for infrared cameras, hazmat detection devices, modern breathing apparatuses, improved training and physical fitness programs, new turnout gear, fire trucks, and interoperable communications equipment, to name but a few items. The SAFER program ago is a vital complement to the Fire Grant program because insufficient staffing, defined by the National Fire Protection Association as fewer than four firefighters per fire truck, is a very real problem for far too many of the nation's career and volunteer fire departments.
Source: http://somd.com/news/headlines/articles/2046.shtml

[Return to top]

Information Technology and Telecommunications Sector

22. *May 18, Washington Technology* — **Survey: homeland security IT initiatives nearly completed.** Most homeland security IT initiatives may be near completion for federal agencies governmentwide, according to the new 2005 Federal IT Marketing Report published by Market

Connections Inc. The findings are based on a survey of 600 federal IT professionals, including 181 from Defense agencies, 44 from the Department of Homeland Security and 375 from other civilian agencies. Anti−terrorism IT projects appear to be in the final stages. Forty−six percent of the respondents said they had completed at least 75 percent of their homeland security IT initiatives. The five most important homeland security IT initiatives reported were IT security, physical security, disaster recovery, threat assessments and threat response. The least important IT initiatives were information−sharing with the public, support of state and local agencies, information−sharing between agencies and adapting existing technology, the report said.
Report: http://www.marketconnectinc.com/IT_report.html
Source: http://www.washingtontechnology.com/news/1_1/daily_news/2619 9−1.html

23. *May 18, International Herald Tribune* — **Computer virus may be aimed at German election.** The creator of a computer Trojan horse that unleashed a torrent of far−right spam e−mail messages in Germany on Tuesday, May 17, may be trying to influence the outcome of the election Sunday, May 22, in North Rhine−Westphalia, a German software expert said. Computers infected with the so−called Sober.q Trojan horse unwittingly sent thousands of spam e−mails bearing links to the Website of the National Democratic Party (NPD), a party that espouses "Germany for Germans," the death penalty for some drug dealers and an end to asylum−seeker rights. "This is most likely connected to the election coming up on Sunday," said Christoph Hardy, a spokesperson for the German unit of Sophos, a British anti−virus software company. "It was probably generated by someone who is sympathetic to the far−right, trying to create anger and a protest vote in Sunday's election." Sober.q was reported to have spread widely around Europe and also to have infected computers in the United States and Asia. The originator of the Trojan horse was most likely German because the programming language used to create the Trojan horse was German, as was the language in the e−mail.
Source: http://www.iht.com/articles/2005/05/17/business/virus.php

24. *May 17, SecurityFocus* — **Microsoft IPV6 TCPIP loopback LAND denial of service vulnerability.** The Microsoft Windows IPV6 TCP/IP stack is prone to a "loopback" condition initiated by sending a TCP packet with the "SYN" flag set and the source address and port spoofed to equal the destination source and port. When a packet of this type is handled, an infinite loop is initiated and the affected system halts. A remote attacker may exploit this issue to deny service for legitimate users. There is no solution at this time.
Source: http://www.securityfocus.com/bid/13658/info/

25. *May 17, SecurityFocus* — **Microsoft HTML Help Workshop memory corruption vulnerability.** The Microsoft HTML Help Workshop compiler tool, 'hhc.exe', is prone to a memory corruption vulnerability. Immediate consequences of exploitation of this issue result in an application crash; this would not be considered a vulnerability. However, it may be possible to subtly manipulate the contents of the affected registers so that an exploitable code path is reached. There is no solution at this time.
Source: http://www.securityfocus.com/bid/13668/discussion/

26. *May 17, FrSIRT* — **PServ command execution and information disclosure vulnerabilities.** Multiple vulnerabilities were identified in PServ, which may be exploited by attackers to execute arbitrary commands or disclose sensitive information. The first issue is due to an input validation error when handling specially crafted HTTP requests containing directory traversal

sequences, which may be exploited by a remote attacker to disclose the source code of cgi scripts or read arbitrary files outside of the webroot directory. The second flaw is due to a buffer overflow error when processing a specially crafted "completedPath" variable, which may be exploited by attackers to execute arbitrary commands with the privileges of the web server. There is no solution at this time.
Source: http://www.frsirt.com/english/advisories/2005/0555

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 (−−−), 135 (epmap), 27015 (halflife), 10684 (−−−), 53 (domain), 113 (auth), 1025 (−−−), 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

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) 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