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

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

Daily Highlights

- The Associated Press reports air traffic controllers were unable to hear pilots for about 20 minutes due to an equipment malfunction at Tampa International Airport, and backup handheld radios were used for about five hours before the system was restored. (See item 7)
- Reuters reports a federal judge has ruled Washington, DC, can ban hazardous rail shipments through the city on security grounds until the federal government devises a solution to safeguard the capital. (See item 8)
- The Department of Homeland Security has announced that for the third season in a row, it is joining Minor League Baseball to promote emergency preparedness, by featuring Ready campaign information in their ballparks. (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; 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. *April 18, Bloomberg* — **More power blackouts are likely due to lack of investment, according to report.** Power blackouts similar to those in the U.S. East Coast, Italy and the UK two years ago are likely to be repeated around the world because of insufficient investment and aging power plants, PriceWaterhouseCoopers said. About $12.7 trillion of investment is needed through 2030 to meet an expected doubling in electricity consumption, a report by consultants

at PriceWaterhouseCoopers said. That total is higher than the estimated $10 trillion spending on electricity called for by the International Energy Agency during the same period. “Blackouts are expected to become more frequent,” according to the report, which was based on a survey of 119 investors and executives at utilities in 36 countries. “Two−thirds of utility respondents believe the likelihood of blackouts will increase or remain the same. Only a quarter think it will reduce,” according to the report. Security of supply is a major concern for 72 percent of the utility industry executives surveyed, up from 65 percent last year, the report said. North America will need about $3.4 trillion of investment through 2030, more than any other region, because it's also the biggest energy consumer, the report said.
Utilities Global Survey 2005:
http://www.pwcglobal.com/Extweb/pwcpublications.nsf/docid/E10D9F24873B0C2485256FD90052C6C9#top
Source: http://www.bloomberg.com/apps/news?pid=10000085&sid=a6L1TI_U75ws&refer=europe

2. *April 18, The Day (CT)* — **Nuclear reactor shut down by malfunction.** A computer detected low pressure in the steam system of the Millstone three reactor at Millstone Power Station, located in Waterford, CT, on Sunday, April 17, forcing the plant into automatic shutdown, plant and federal officials said. The cold manual shutdown that followed led to a second complication when a safety relief valve wouldn't close properly, said Pete Hyde, spokesperson for Millstone owner Dominion Nuclear Connecticut. The shutdown of the Millstone three reactor means that all three of the nuclear complex's reactors are closed and not generating any electricity. The older reactors, Millstone one and two, were not affected by Sunday's incident. Unit one is closed and in the process of being decommissioned. Unit two is temporarily shutdown for refueling which takes several weeks. It is unknown when Millstone three could begin operating again. “We're going to do an extensive investigation of all the systems involved,” Hyde said. “We have to fix the problem and we're not going to bring (Millstone three) back online until we're sure we've fixed the problem. It's a little more serious than some of the things we've been through in the past and it requires a higher level of scrutiny,” said Hyde.
Source: http://www.theday.com/eng/web/news/re.aspx?re=FAA98755−99C1−4A40−B13E−465597D31019

[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. *April 18, Vvnunet.com* — **Consumers make it easy for e−commerce hackers.** UK consumers are unwittingly helping hackers target e−business firms by leaving themselves unprotected from spam, key−logging and phishing attacks, research has claimed. A newly published poll of 11,000 UK residential e−mail users and small to medium sized businesses (SMEs) found that users are the weakest link for banks, retailers and other online businesses, offering hackers easy access. The study, commissioned by e−mail filtering managed service provider Checkbridge, indicated that almost two thirds of consumers and SMEs have no anti−spam filtering installed. "Market debate for some time now has centered on the vulnerability of corporations. Consumers and SMEs, and their interaction with corporations, are a neglected and critical link in the national armory," said John Turley, managing director at Checkbridge. "It is in the banks' and retailers' interests to get consumer protection right, whether by approaching government, endorsing those ISPs that offer sufficient protection or paying for secure telecoms infrastructure (e.g. VPNs) for their client base."
Checkbridge: http://www.checkbridge.com
Source: http://www.vnunet.com/news/1162529

4. *April 18, The Pantagraph (IL)* — **University changing identity card system.** Illinois State University (ISU) is revamping its ID system with hopes it will keep identity thieves at bay. Nearly 25,000 new campus IDs −− the most visible piece of an estimated $250,000 identification−system conversion −− will be distributed this month and become effective June 1. "We reviewed how ubiquitous the Social Security number had become" and determined a new system was necessary, said Bill Cummins, university data administration. The conversion is in line with a national trend to eliminate Social Security number usage in campus information systems. At ISU, a task force established in fall 2003 presented findings 18 months ago that led to plans for June's conversion. Illinois State's ID conversion has been quite an undertaking, said Cummins. Not only does the university need to trade out about 25,000 cards, but university staff must remove Social Security numbers from millions of records in ISU computer files, he said. His staff and others are planning for most of the ID conversion to take place Memorial Day weekend, and to use the summer months to work out kinks. ISU still will collect Social Security numbers for business reasons. However, officials will limit what university computer files include such data.
Source: http://www.pantagraph.com/stories/041805/new_20050418027.sht ml

5. *April 18, Reuters* — **Disclosure of bank data may not aid the fight against terrorism.** A plan to force banks into disclosing hundreds of millions of wire transfers to help fight terrorist financing would overwhelm bankers and regulators and add questionable value to the war on terrorism, experts and officials say. The proposal is being studied by the U.S. Treasury and would grant the government unprecedented access to banking records. Banks wire more than $6 trillion across the globe each day, the bulk of it in and out of the United States. While counterterrorism officials are eager to tap into this financial information, some officials, bankers and experts question whether authorities can actually glean pertinent information from the flood of data, while protecting the privacy of banking clients. "The big provisos are whether that data can be obtained in a cost−effective way that doesn't overburden the private sector, doesn't choke the government, and in a way that it can be ... used without running roughshod over privacy and civil liberties concerns," said Joseph Myers, a former National Security Council official under President Bush. Many officials and experts, including Myers, say wire transfers might contain useful information to track down terrorists and believe the idea of

reporting some of those flows merits study, as long as the challenges are clear.
Source: http://www.washingtonpost.com/wp−dyn/articles/A62643−2005Apr 18.html

6. *April 17, The News Journal (DE)* — **Newlyweds targeted in identity theft scam.** The latest identity theft scam targets newlyweds, said New Castle County, DE, Clerk of the Peace Ken Boulden. The unwitting couple receives a letter saying they are required to register their name change with the federal government. They are asked to supply a wealth of personal information −− address, birth date, even Social Security number. A fee of $15 to $20 is needed, payable by check or credit card. "Not only have you given them your entire life on this registration card, you've given them copies of your signature, your routing number or your bank account number, and you're paying them to take it," Boulden said. "There is no federal or state requirement or law that mandates that you register or record your change of name after marriage, period," he said. Boulden first learned of this relatively new scam while attending a conference. He said he was surprised to hear of it, and even more surprised that newlyweds have started calling his office to ask about mailings from entities with official−sounding names such as National Record Service Corp. and U.S. Record Service Corp.
Source: http://www.delawareonline.com/newsjournal/local/2005/04/17ne wlywedstarget.html

[Return to top]

Transportation Sector

7. *April 18, Associated Press* — **Air traffic controllers forced to use backup handheld radios.** Air traffic controllers were unable to hear pilots for about 20 minutes due to an equipment malfunction at Florida's Tampa International Airport. Backup handheld radios were used for about five hours before the system was restored. The tower's radar worked continuously during the outage Saturday, April 16, and officials said no planes were in danger or diverted to other airports. Some planes waiting to take off were delayed briefly on the ground until controllers switched to the radios. The Federal Aviation Administration extended the space between departing and arriving flights as a precaution. Rich Reid, an air traffic control operations manager, said the problem was "very minor in the whole scheme of things."
Source: http://www.local6.com/news/4388000/detail.html

8. *April 18, Reuters* — **Court permits District to block hazardous rail shipments.** Washington, DC, can ban hazardous rail shipments through the city on security grounds until the federal government devises a solution to safeguard the capital, a federal judge ruled on Monday, April 18. U.S. District Judge Emmet Sullivan denied a bid by freight rail giant CSX Corp. to block a 90−day prohibition on freight cars hauling flammable gases and explosives from moving within two miles of the U.S. Capitol. The ban is scheduled to take effect on Wednesday, April 20. City officials fear hazardous chemicals and other substances could be inviting targets for attacks, and imposed the ban out of frustration with federal security efforts. CSX has two lines running through the Washington area. The District City Council considered studies that an attack on a train or truck carrying certain hazardous materials in or close to Washington could cause thousands of deaths and billions of dollars in economic damages. The case has attracted the attention of communities concerned with protecting themselves from an attack on rail tankers loaded with toxic materials.
Source: http://www.reuters.com/newsArticle.jhtml?type=domesticNews&s toryID=8214914

9. *April 18, Bloomberg* — **Amtrak runs Acela train with repaired brakes.** Amtrak, the U.S. national passenger railroad, ran a single Acela high−speed train from New York to Washington, DC, on Monday, April 18, while 19 other trains were kept out of service because of brake problems. Spokesperson Clifford Black said the railroad hopes to put a second set of equipment into service later this week. Amtrak got the train, which can carry 300 passengers, back in service by using undamaged brakes from other trains. Amtrak suspended the service, which reaches speeds of 150 miles per hour, on Friday, April 15, after finding 300 damaged brakes out of 1,440 on trains built by Bombardier Inc. of Montreal and France's Alstom SA, for $1.2 billion. Acela made its debut in 2000 almost a year late because of mechanical flaws, and was idled for weeks in 2002 to fix a shock absorber defect. Chief Operating Officer Bill Crosbie said last week that it could be two months before all Acelas are repaired. Amtrak's weekday schedule includes 15 round trips between New York and Washington and 11 between Boston and New York. Substitute equipment is being used to cover about half of those Acela trips, Black said.
Source: http://www.bloomberg.com/apps/news?pid=10000103&sid=aLAvxKpRamjk&refer=us

10. *April 14, Transportation Security Administration* — **Explosives detection trace portal deployed to San Francisco International.** Starting Thursday, April 14, a new explosives detection trace portal was used to screen passengers at the San Francisco International Airport (SFO) in the International Terminal at the Concourse G security checkpoint, the Transportation Security Administration (TSA) announced. The equipment is part of a pilot program to test and evaluate the trace portal for screening passengers for explosives. At SFO, some passengers will be directed by the TSA screeners to step into the trace portal. Passengers will stand still for a few seconds while several “puffs” of air are released. The portal will collect and analyze the air for traces of explosives and a computerized voice will tell passengers when to exit. Even as the pilot program continues, TSA has allocated $28.3 million to purchase and install an additional 147 trace portals. TSA is currently developing a purchase and deployment plan to have the equipment in airports by January 2006. Once the plans are finalized, TSA will announce the next group of airports to receive the equipment.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 011816c

[Return to top]

Postal and Shipping Sector

11. *April 18, Pitney Bowes Inc.* — **Pitney Bowes acquires selected assets of Fala Sorting Services, Inc.** Pitney Bowes Inc., on Monday, April 18, acquired selected mail stream and presort assets of Fala Sorting Services, Inc. (FSS), a subsidiary of Fala Direct Marketing, Inc. FSS provides domestic and international presorting and commingling mailing services for mail produced in the greater New York area. The FSS assets will be integrated with the company's Mail Services operations which include PSI Group specializing in first and standard class domestic letter mail, and International Mail Express (IMEX) which provides international outbound mail services. Fala Direct Marketing will continue to provide lettershop services with a greater emphasis on its core business and its expanding graphics and printing solutions. Fala Direct Marketing and the company have also signed a long−term marketing agreement to

provide Fala's customers with access to pre−sort and international mail services through the Pitney Bowes Mail Services national network.
Source: http://biz.yahoo.com/prnews/050418/nym229.html?.v=4

[Return to top]

Agriculture Sector

12. *April 18, Mail Tribune (OR)* — **Disease threatens hatchery steelhead.** Discovery of a potentially deadly disease among adult winter steelhead at Oregon's Cole Rivers Hatchery has prompted stepped−up efforts to ensure it is not spread to more than 300,000 steelhead eggs set to be spawned there this spring. The virus Infectious Hematopoietic Necrosis (IHN) was found in adult hatchery winter steelhead collected recently from the Rogue and Applegate rivers and spawned at Cole Rivers, which is on the upper Rogue. Tests of ovarian fluids in the spawned fish came back positive for IHN, a somewhat mysterious disease that occurs naturally in streams and does not always lead to fish die−offs. The disease can be spread among adult salmon and steelhead, but does not harm mammals. It rarely is passed from spawning adults to their eggs, but it can be spread readily through the hatchery's water supply. So far, IHN has not been discovered in any other fish or eggs there.
Source: http://www.mailtribune.com/archive/2005/0418/local/stories/0 2local.htm

13. *April 18, Associated Press* — **Fungus, energy costs complicate crop choices.** Deciding whether to plant corn or soybeans usually isn't difficult. Most grain farmers tend to stick with their long−planned rotation of beans one year and corn the next. The decision has been complicated this year by the threat of soybean rust, a fungus that could hurt production, and high nitrogen and propane costs that could reduce corn profits. "I'm sure everyone thought about this," said Ellen Joslin, who farms about 1,000 acres near Sidney in western Ohio. "Energy prices are going through the roof. That's almost more of a concern than soybean rust." Jim Beurelein, an agronomist with Ohio State University's Extension program, said a number of farmers were going to grow a lot more corn until costs rose. "On the whole, it's pretty much going to be a wash," he said. Soybean rust has the potential to cause millions of dollars in damage. The fungus, spread by wind−borne spores, has not caused any real damage in the U.S. yet, but it cost farmers in Brazil about one billion dollars last year in crop losses and fungicide treatment. High natural gas prices have made the use of nitrogen−based fertilizer much more costly for corn growers. Nitrogen is made from natural gas.
Source: http://www.ledger−enquirer.com/mld/ledgerenquirer/business/1 1421649.htm

[Return to top]

Food Sector

14. *April 15, Wichita Business Journal (KS)* — **Cargill purchases Canadian beef processing plant.** Cargill Ltd. has reached an agreement to purchase beef processing and related assets of Better Beef Ltd, based in Ontario, Canada. Cargill Ltd. is part of Cargill, an international meat and food processing giant. No price was disclosed on the transaction, which was announced Friday, April 15.

Source: http://www.usagnet.com/story−national.cfm?Id=404&yr=2005

[Return to top]

Water Sector

15. *April 18, Associated Press* — **East Providence residents told to boil water due to bacteria.** East Providence, RI, residents are being advised to boil their water for at least one minute before using it due to the presence of harmful bacteria. Sunday, April 17, health officials found fecal coliform bacteria in East Providence's public water supply. The bacteria indicates the water may be contaminated with human or animal waste. Microbes in those wastes may cause health problems including diarrhea, cramps, nausea and headaches. The microbes pose a special risk for infants, young children and those with severely compromised immune systems. Boiled or bottled water should be used for drinking, making ice, brushing teeth, food preparation and bathing infants until further notice.
Source: http://www.eyewitnessnewstv.com/Global/story.asp?S=3220862&n av=F2DOYlAP

[Return to top]

Public Health Sector

16. *April 18, Reuters* — **Vietnam sees a long fight against bird flu.** The bird flu virus which has killed 36 people in Vietnam may not be contained until 2007 because the way it is spreading still baffles experts, officials said on Monday, April 18. The government aims to contain the H5N1 virus by 2006 or 2007 and eliminate it by 2010, Deputy Agriculture Minister Bui Ba Bong said. Other senior officials said current knowledge about the virus, which has been at its worst during the cool season between December and March in each of the last two years, meant the fight would be a tough one. "This is a new, extremely dangerous disease which contemporary knowledge in our country and internationally has not been able to explain properly," Deputy Prime Minister Nguyen Tan Dung said. He told health, agriculture officials, and foreign experts it was still not known for sure how the virus was transmitted from water fowl, which can carry it without getting sick, to poultry and then to people. "There are cases where a healthy person carries the virus without showing clinical symptoms, which has made the risk of spreading the virus in the community greater," Deputy Health Minister Tran Chi Liem said.
Source: http://www.reuters.com/newsArticle.jhtml?storyID=8210641&typ e=worldNews

17. *April 18, Agence France Presse* — **Angola's Marburg death toll rises to 235.** The death toll from the Marburg virus epidemic rose to 235 in Angola on Sunday, April 17, with some 500 people under surveillance after coming in contact with the Ebola−like virus, the health ministry and the World Health Organization (WHO) said. Health officials are treating a total of 257 cases of the virus that has claimed 219 lives in the northern province of Uige, the epicenter of the outbreak that was first detected in October, according to a statement from the ministry and the WHO. An additional 513 people are under surveillance, it added. WHO experts said last week that there was no end in sight for the epidemic, the worst outbreak ever of the virus first detected in 1967 when German laboratory workers in Marburg were infected by monkeys from

Uganda.
Source: http://www.reliefweb.int/rw/RWB.NSF/db900SID/MHII−6BK3SS?Ope nDocument

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

18. *April 16, City of Burnsville (MN)* — **City better prepared to deal with disaster after emergency management exercise.** Should a disaster such as a flood, tornado or other tragic event impact Burnsville, MN, city services will not be alone in responding. An Emergency Management Drill held during the morning hours on Saturday, April 16 simulated a tornado touchdown in a Burnsville neighborhood and allowed for a real life training for City Police and Fire responders, Fairview Ridges Hospital and other emergency response agencies, including a citizen based group of responders called the Mobile Volunteer Network. Over 100 volunteers were involved in the four hour training which was held in three locations: Burnsville City Hall/Police Station, Fairview Ridges Hospital, and a neighborhood located just east of Red Oak Park along Baypoint Drive and Summerset Lane. Residents can get a look behind the scenes at the training exercise by viewing a special video documentary on the training session that will be shown on a local cable channel during the month of May.
Source: http://www.ci.burnsville.mn.us/government/4−16Drill.htm

19. *April 14, Department of Homeland Security* — **Department of Homeland Security and Minor League Baseball team up to promote emergency preparedness.** The Department of Homeland Security announced Thursday, April 14, that for the third season in a row, it is joining Minor League Baseball to promote emergency preparedness. During the 2005 season, 48 teams across the nation will educate and encourage their fans to prepare for emergencies in their homes, businesses and schools by featuring Ready campaign information in their ballparks, beginning April 14, 2005. Many teams will take part in the effort by featuring Ready campaign television or radio public service announcements in their ballparks and/or game programs. Ready asks citizens to do three key things: get an emergency supply kit, make a family communications plan, and be informed about the different types of emergencies that could occur and their appropriate responses. By providing this important information, teams are helping to prepare fans and their communities to respond to potential emergencies. Boy Scout troops across the nation will also take part in the effort again this season by distributing Ready brochures during selected Minor League Baseball games. Individuals interested in receiving a "Get Ready Now" brochure may call 1−800−BE−READY or visit Ready.gov for more information. To get involved, contact the local Citizen Corps Council: http://www.citizencorps.gov/
Source: http://www.dhs.gov/dhspublic/display?content=4463

[Return to top]

Information Technology and Telecommunications Sector

20. *April 18, IDG News Service* — **EU task force to study IT critical infrastructure.** The European Union has set up a task force to explore what its 25 member states are doing to combat cyberthreats against the region's critical infrastructure. As part of the EU's Critical Information Infrastructure Research Coordination (CI2RCO) project, announced Friday, April 15, the task force aims to identify research groups and programs focused on IT security in critical infrastructures, such as telecommunications networks and power grids. "We want to bring together experts across the European Union, learn more about their programs and how we can cooperate in curbing what we view as a global problem," said Paul Friessem, a director at the Fraunhofer Institute for Secure Information Technology (SIT), one of the organizations in the European task force. "We also intend to collaborate with experts outside the EU, in particular in the U.S., Canada, Australia and even possibly Russia." One of the problems facing the task force is convincing parties to divulge information that some governments view as critical to their national security. The task force will also ask the critical infrastructure players about their requirements. The plan is to submit an overview of the situation to the European Commission over the next few months.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,101160,00.html

21. *April 15, IDG News Service* — **Vendors call for more government cybersecurity focus.** The U.S. government needs to get more serious about cybersecurity, but Congress should look at broader ways to combat security problems than focusing on bills that address specific issues such as spam or spyware, a group of executives from IT security product vendors said last week. Members of the Cyber Security Industry Alliance (CSIA), meeting in Washington, DC, Thursday, April 14, repeated their call for Congress to create an assistant secretary for cybersecurity position at the Department of Homeland Security. Members of the year−old CSIA, meeting as a rash of data breaches have been announced in recent months, said they committed this week to helping Congress and administration officials understand cybersecurity issues. While most CSIA executives said they would welcome the right kind of cybersecurity legislation, not all technology companies favor new laws. Private companies should have time to find their own solutions to data breaches and explain their efforts to Congress, said Howard Schmidt, chief security strategist at eBay, during a forum on ID theft at the Washington think tank the Center for Strategic and International Studies Friday, April 15.
CSIA Website: https://www.csialliance.org/home
Source: http://www.nwfusion.com/news/2005/0415vendocall.html

22. *April 15, eWeek* — **Education network seeks to become nation's largest Wi−Fi hot spot.** Although students and faculty members at virtually all universities and many school systems routinely access the Internet through their local networks today, gaining access from remote campuses is difficult. That's about to change through an initiative called Education First, a cooperative effort of two educational management organizations, based in Minnesota, and two Massachusetts−based wireless technology companies working to turn the entire educational community into one giant coast−to−coast hot spot. According to Jo Boettcher, chief operating officer of the Broadband Alliance, one of the sponsoring educational organizations, the effort is the latest development in the fast−moving trend toward convergence on the nation's campuses. Education First, she said, "allows a virtual network so educators can share information as they

have mobility." Interuniversity connectivity is not new. It's been happening on many campuses −− but not easily. Participating institutions will join the Education First service through The National Joint Powers Alliance, a nonprofit nationwide purchasing clearinghouse for schools and universities. Education First will also offer the program to schools, K−12, and will work to acquire Wi−Fi networks at reduced costs to those that don't have them.
Source: http://www.eweek.com/article2/0,1759,1787033,00.asp

23. *April 14, Government Accountability Office* — **GAO−05−567T: Department of Homeland Security Faces Challenges in Fulfilling Statutory Requirements (Testimony).** For many years, the Government Accountability Office (GAO) has reported that poor information security is a widespread problem that has potentially devastating consequences. Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that made them vulnerable to attack, Congress passed the Federal Information Security Management Act of 2002 (FISMA). This testimony discusses Department of Homeland Security's (DHS) progress and challenges in implementing FISMA. DHS has made progress in implementing key federal information security requirements, yet it continues to face challenges in fulfilling the requirements mandated by FISMA. In its fiscal year 2004 report on FISMA implementation, DHS highlights increases in the majority of the key performance measures (developed by the Office of Management and Budget (OMB) to track agency performance in implementing information security requirements), such as the percentage of agency systems reviewed and percentage of employee and contractor personnel who received security awareness training. However, DHS continues to face significant challenges in meeting most statutory information security requirements. For example, DHS has yet to develop a complete and accurate inventory or an effective remediation process.
Highlights: http://www.gao.gov/highlights/d05567thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−567T

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: Microsoft has released a Security Bulletin Summary for April, 2005. This summary includes several bulletins that address vulnerabilities in various Windows applications and components. Exploitation of some vulnerabilities can result in the remote execution of arbitrary code by a remote attacker.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 41170 (−−−), 4662 (eDonkey2000), 6346 (gnutella−svc), 1026 (−−−), 139 (netbios−ssn), 53 (domain), 1027 (icq), 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

24. *April 18, NapaNews (CA)* — **Surveillance of public areas increases.** Chicago is working on plans to link more than 2,000 surveillance cameras across the city into a network that would use computer software to alert authorities to suspicious activities. In Los Angeles, the police department recently deployed a camera surveillance system to identify, track and record criminal activity in certain areas of the city. The system is equipped with "intelligent" video capabilities and facial recognition software. The "intelligent" software identifies human movement within designated areas which enables officers to remotely identify and monitor suspicious activities. In New Orleans, cameras are not routinely monitored; video is stored for a brief period, to be watched if a crime is reported. Only a few qualified officers have access to the video, and they look at it only in response to a specific report. The first cameras were installed in October, initially in drug dealing hot spots. So far, about 240 of the proposed 1,000 cameras are now in operation.
Source: http://www.napanews.com/templates/index.cfm?template=story_full&id=1412E9A8−7C58−4C28−ACA2−9B45D72D0820

[Return to top]

General Sector

25. *April 15, Associated Press* — **Controversial terrorism database shuts down.** A three−year−old crime and terrorism database that came under fire for sharing and collecting personal information was closing down Friday, April 15, because a federal grant ran out. Elements of the Multistate Anti−Terrorism Information Exchange −− Matrix −− may live on if individual states decide to fund it on their own, said Bob Cummings, executive vice president for the Institute for Intergovernmental Research in Tallahassee, which helped coordinate the Matrix network. Matrix was down to four participants −− Pennsylvania, Florida, Ohio and Connecticut –− after several states opted out due to privacy concerns, legal issues or cost. It operated with grant money from the Departments of Justice and Homeland Security, but that funding expired Friday. Matrix helped in terror−related investigations and to identify and locate suspects in violent crimes, drug−related cases, home invasions and other investigations, law enforcement officials said. In Pennsylvania, the system had 1.9 million queries since July 2003. The database drew immediate criticism from privacy rights groups, including the American Civil Liberties Union (ACLU), which argued that it provided unprecedented access to details about innocent people, including credit histories, marital history, fingerprints and Social Security numbers.
Matrix: http://www.matrix−at.org/
Source: http://www.siliconvalley.com/mld/siliconvalley/news/editoria l/11405499.htm

[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 and assessment 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