



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

Current  
Nationwide  
Threat Level is  
**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS  
[For info click here](http://www.dhs.gov/)  
<http://www.dhs.gov/>

## Daily Highlights

- U.S. Immigration and Customs Enforcement agents on Friday arrested 14 illegal aliens, including one fugitive alien with an outstanding deportation order, as part of an ongoing investigation into an illegal worker scheme at Logan International Airport in Boston. (See item [10](#))
- The Environmental Protection Agency's Inspector General said Thursday that the agency hasn't ensured the reliability, timeliness and efficiency of air sampling by BioWatch, a \$129 million bioterrorism early warning system. (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. *March 25, Associated Press* — **Energy consumers in the Northwest urged to conserve power.** Without robust efforts by consumers to conserve electricity in coming months, utilities throughout the Northwest could see an across-the-board rate increase because of drought, energy officials said Thursday, March 24. "If we don't change anything, we are heading toward a rate increase. What we're talking about is trying to change our destiny," said Bonneville Power Administrator (BPA) Steve Wright, who was joined by nine other energy officials from various utilities in urging conservation. Dry weather affects power generation in the Northwest — Washington, Oregon, Idaho and parts of Montana — more than other areas because the

region is highly dependent on the energy produced by its dams. Roughly 60 percent of the energy produced in the region is hydroelectric, compared to 15 percent nationally, said Wright. Water levels are now at 63 percent of normal, making this one of the worst years on record. Unlike in 2001, the current energy crunch will not lead to blackouts, officials said. Instead, its impact stands to be financial. In most years, the BPA sells its surplus power to energy-strapped states. This year, it expects to have to buy power.

Source: <http://www.idahostatesman.com/apps/pbcs.dll/article?AID=/20050325/NEWS02/503250311/1029>

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

2. *March 26, Express–News (TX)* — **San Antonio chemical spill spurs reverse–911 calls.** Bexar County sheriff's dispatchers in San Antonio, TX, used the reverse–911 system, an emergency phone message sent en masse to residents of a particular area, on Friday, March 25, to notify residents of a Northeast Side neighborhood to stay inside their homes while firefighters cleaned up spilled chlordane. Chlordane, a pesticide formerly used on crops, lawns and termites, was banned by the Environmental Protection Agency in 1988 because of concern about it damaging the environment and human health. No one reported being sick from the chemical.

Source: [http://www.mysanantonio.com/news/metro/stories/MYSA032605.3B\\_chem\\_spill.173d9b725.html](http://www.mysanantonio.com/news/metro/stories/MYSA032605.3B_chem_spill.173d9b725.html)

[[Return to top](#)]

## **Defense Industrial Base Sector**

Nothing to report.

[[Return to top](#)]

## **Banking and Finance Sector**

3. *March 25, Government Technology* — **Information Technology Association of America announces strategy for protecting consumer data.** The Information Technology Association of America (ITAA) on Thursday, March 24, announced a six–point strategy to enhance the privacy and security of consumer data. ITAA also called for all involved in assuring the privacy of consumer records, including government agencies, the financial services industry, data aggregators and other technology firms, to work together in implementing the strategy. ITAA's plan focuses on three areas: improving law enforcement powers and capabilities to focus on the lawbreakers; reducing the number of breaches; and notifying affected individuals in the event personal data are improperly disclosed or obtained. "Custodians of data, government and individuals all have a share of the responsibility in protecting personally identifiable information and other sensitive data and assuring its appropriate use," said ITAA President Harris N. Miller. Strategy:

[http://www.ita.org/eWeb/Dynamicpage.aspx?webcode=PRTemplate&wps\\_key=feb66fec-d4dc-4253-b628-8c14b1a0e0b1](http://www.ita.org/eWeb/Dynamicpage.aspx?webcode=PRTemplate&wps_key=feb66fec-d4dc-4253-b628-8c14b1a0e0b1)

Source: <http://www.govtech.net/news/news.php?id=93481>

4. **March 25, Internetnews.com — Phishing attacks increase in numbers and sophistication according to industry group.** Pharming, or “phishing without a lure,” is an increasingly common attack style, the Anti-phishing Working Group said in its February Phishing Activity Trends report. Pharming is more sophisticated than phishing and harder to detect. "Pharming is a class of navigational attacks that seeks to corrupt the navigational infrastructure the consumer sees, to trick him into going places he's really not supposed to or obscure the fact he's visiting places he didn't want to go," said Peter Cassidy, secretary general of the Anti-Phishing Working Group. In these schemes, crooks surreptitiously slip malicious code into someone's computer that modifies the host's file; when the person types in a URL and the browser checks the host file for the IP address, the malware will send the person off to a bogus site, Cassidy said. One alarming trend is phishers' move downscale. While they used to target the largest companies and major financial institutions, they've begun mimicking regional banking sites and smaller Web retailers. According to the report, 13,141 new, unique phishing e-mail messages occurred in February 2005, more than a two percent increase over January. The average monthly growth rate in attacks since July 2004 was 26 percent. Report: [http://antiphishing.org/APWG\\_Phishing\\_Activity\\_Report\\_Feb05.pdf](http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf)  
Source: <http://www.internetnews.com/security/article.php/3493046>
  
5. **March 24, Government Accountability Office — GAO-05-262: Information Security: Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data (Report).** The Securities and Exchange Commission (SEC) relies extensively on computerized systems to support its financial and mission-related operations. As part of the audit of SEC's fiscal year 2004 financial statements, the Government Accountability Office (GAO) assessed the effectiveness of the commission's information system controls in protecting the integrity, confidentiality, and availability of its financial and sensitive information. GAO recommends that the SEC Chairman direct the Chief Information Officer to take several actions to fully develop and implement an effective agencywide information security program. In commenting on a draft of this report, SEC agreed with GAO's recommendations. SEC plans to address the identified weaknesses and indicated that significant progress is already being made to address them. Highlights: <http://www.gao.gov/highlights/d05262high.pdf>  
Source: <http://www.gao.gov/new.items/d05262.pdf>
  
6. **March 24, Vnunet.com — UK residents susceptible to identity theft.** A survey of Londoners has found that 92 percent of them will give a stranger all the information required to steal their identity. Researchers offering the chance to win theater tickets questioned over 200 people. Over the course of a three-minute interview the researchers asked a series of questions about theater habits but also extracted names, addresses, school history and the names of parents and siblings. "The results of the survey are disturbing to say the least, but they do highlight the need to raise public awareness of identity theft, what it actually means, how it can happen and the potential consequences," said Detective Inspector Chris Simpson, head of Scotland Yard's Computer Crime Unit. During the survey 98 percent of people gave out their addresses, 92 percent revealed their mother's maiden name and pet's name, 96 percent gave their home phone number and the same proportion gave the name of their first school. This information is all that would be required to open a bank account in their names.

Source: <http://www.vnunet.com/news/1162160>

7. *March 24, TechWeb News* — **Banking and retail industries urged to fight identity theft.** Banking and retail industries could do more to make online transactions more secure. For example, they could develop better methods for verifying that people conducting transactions are who they say they are, a research firm said Thursday, March 24. "The best defense is to be able to prevent a thief from actually using the data once they secure it," Financial Insights analyst Sophie Louvel. Also, banks, in particular, may want to consider providing free services to help victims deal with the aftermath, such as correcting credit reports that may list the fraudulent activities. Recovery services available for a fee, such as Identity Theft 911, could act as models for the banks. "They can be more proactive with identity-theft services that help victims recover," Louvel said. Report Overview: <http://www.financial-insights.com/FI/getdoc.jsp?containerId=FIN1586>  
Source: <http://www.techweb.com/wire/security/159905624>

[[Return to top](#)]

## **Transportation Sector**

8. *March 25, Transportation Security Administration* — **TSA officials to deploy additional explosives trace portals at five airports.** The Transportation Security Administration (TSA) announced Friday, March 25, it will deploy Explosives Detection Trace Portal machines to the following airports by the end of May 2005: Miami International, San Francisco International, Phoenix Sky Harbor International, Boston's Logan International, and Los Angeles International. Under the program, select passengers will be directed by the TSA screeners to step into the trace portal. These passengers will remain in the portal for a few seconds while several "puffs" of air are released. The portal will then analyze the air for traces of explosives and a computerized voice will tell the passenger when to exit. With this latest deployment, TSA will then have trace portals in 14 airports by the end of May 2005. TSA Website: <http://www.tsa.gov/public/>  
Source: [http://www.tsa.gov/public/display?theme=44&content=090005198\\_010edad](http://www.tsa.gov/public/display?theme=44&content=090005198_010edad)
9. *March 25, Reuters* — **FAA orders rudder inspections on some Airbus planes.** U.S. aviation regulators on Friday, March 25, ordered detailed rudder inspections and repairs, if necessary, of certain Airbus planes after the rudder of a Canadian passenger jet nearly fell off this month. Officials within the Federal Aviation Administration (FAA) want operators of the 112 European-made Airbus A310s and A300s registered to U.S. carriers to complete detailed rudder inspections within three months. The planes are flown primarily in the United States by cargo giant FedEx Corporation. American Airlines also operates some A300s. The tests include visual checks and a tap test, which is an audio analysis. The directive stems from a March 6 in-flight incident in which a Canadian charter A310 lost part of its rudder. The Air Transat flight from Cuba to Quebec City with 270 people aboard returned safely to Cuba. FAA Website: <http://www.faa.gov/>  
Source: <http://www.reuters.com/newsArticle.jhtml;jsessionid=YQO5ICFR5235CCRBAEOCFEY?type=domesticNews&storyID=8004627>

10. *March 25, Immigration and Customs Enforcement* — **Immigration and Customs**

**Enforcement agents arrest illegal aliens working at airport.** U.S. Immigration and Customs Enforcement (ICE) agents on Friday, March 25, arrested 14 illegal aliens, including one fugitive alien with an outstanding deportation order, as part of an ongoing investigation into an illegal worker scheme at Logan International Airport in Boston, MA. The illegal aliens arrested Friday all worked for Hurley of America, a contract company that provides janitorial services for Logan Airport. The illegal workers all had temporary badges that allowed access to areas beyond where passengers are screened and up to the boarding gates. There is no indication that any of the aliens were involved in any terrorist activity. Thirteen of those arrested will be placed in deportation proceedings. One alien has an outstanding deportation order issued by a federal immigration judge and will be deported. Two are juveniles. All of those arrested are citizens of Brazil. This worksite enforcement action at Logan is part of ICE's "Operation Tarmac," an ongoing nationwide critical infrastructure protection initiative by ICE that targets employers and unauthorized workers who have access to sensitive areas at airports.

Source: [http://www.ice.gov/graphics/news/newsreleases/articles/logan\\_032505.htm](http://www.ice.gov/graphics/news/newsreleases/articles/logan_032505.htm)

11. *March 24, Federal Computer Week* — **DHS Inspector General sees minimal progress for**

**US-VISIT.** Department of Homeland Security (DHS) officials must increase the number of international visitors they track at land-based U.S. ports of entry and ensure that border officials can more quickly verify those visitors' identities, the department's inspector general recommended in a new report. Richard Skinner, DHS' IG, suggested that officials make these changes, among others, to the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program. US-VISIT compiles databases of biographic and biometric information from international visitors to determine whether the travelers pose a terrorist threat. Congress has mandated that US-VISIT must eventually monitor all foreign nationals entering and departing the United States. Although Skinner wrote he was cautiously optimistic that the department would reach its goals, he warned that the program has made only the bare minimum of progress. As of December 31, 2004, DHS officials had deployed US-VISIT at the 50 land ports of entry that receive the most international visitors. Officials at those ports process about 92 percent of all foreign travelers who enter the United States by land. The system will eventually extend to all 165 land ports of entry. Report:

[http://www.dhs.gov/dhspublic/interweb/assetlibrary/OIG\\_05-11\\_Feb05.pdf](http://www.dhs.gov/dhspublic/interweb/assetlibrary/OIG_05-11_Feb05.pdf)

Source: <http://www.fcw.com/article88397-03-24-05-Web>

12. *March 23, Milwaukee Journal Sentinel (WI)* — **Milwaukee under-freeway parking to stay**

**but security concerns could lead to other changes.** More than 1,000 parking spots beneath the ramps and bridges of the Marquette Interchange in downtown Milwaukee, WI won't be eliminated, state officials say. But security concerns could lead to other changes for Wisconsin's bridges, harbors and airports, as state and federal authorities pore over the secret findings of a \$400,000 study of the vulnerabilities of key transportation facilities. The issue came to light after questions about whether downtown parking would be the same after the \$810 million reconstruction of the Marquette Interchange. Milwaukee isn't the only city with parking lots under freeway bridges, because that land is not considered desirable for buildings. A federal ban on such lots would have a nationwide impact. The Department of Homeland Security has never ordered such a ban, however, and no such rule is under consideration, said Brian Doyle, spokesperson for the federal agency.

Source: <http://www.jsonline.com/traffic/news/mar05/312143.asp>

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

## **Postal and Shipping Sector**

**13. *March 25, Associated Press* — Executive board of UPS pilots union approves strike vote.**

The executive board of the pilot union at UPS, the world's largest shipping carrier, has approved holding a strike authorization vote after protracted contract talks between the two sides broke down, the union said Thursday, March 24. The company, however, said talks have not broken down and the union was mischaracterizing the status of negotiations. More talks have been scheduled for May, UPS noted. The two sides have been in federal mediated talks since last June but have not been able to reach agreement on issues involving scheduling, scope, compensation, pension, and benefits. A strike authorization vote allows the union to call a strike without polling its members again, but does not mean that a walkout is imminent. Under the Railway Labor Act, the pilots can't strike while mediated talks are ongoing and no timetable has been set for when the talks will end.

Source: <http://www.nytimes.com/aponline/business/AP-UPS-Pilots.html?oref=login>

**14. *March 24, Houston Chronicle (TX)* — New system in Houston mail center scans for anthrax.**

Houston, Texas' main downtown facility has a new system that can detect anthrax on letters. The city's downtown processing and distribution center had the Biohazard Detection System, BDS, installed March 19, making it the first postal location in the state to get it. The automated system continuously collects air samples as letters move through the machinery. If anthrax is detected, workers are given a visual and audible alert. The system, which is already used in about 75 other processing locations across the U.S., was first put into use in 2003. The system has the capability of being expanded to test for other biochemical substances. The technology will be used on the more than 1.6 million letters collected every day in the city. If an alert does sound, employees and customers will evacuate the building.

Source: <http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/3101614>

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

## **Agriculture Sector**

**15. *March 25, Agricultural Research Service* — Scientists find bacterium can control fire blight disease in tree fruit.**

Agricultural Research Service (ARS) scientists in Wenatchee, WA, are attempting to eradicate *erwinia amylovora*, the bacterium responsible for fire blight, a costly disease of apples, pears, and other tree fruit. Controls include pruning, cultural practices, and spraying infected trees with antibiotics. Resistance to one antibiotic, streptomycin, has emerged in fire blight strains of the Pacific Northwest. Now, as a bio-alternative, ARS plant pathologist Larry Pusey and colleagues are calling on *Pantoea agglomerans* strain E325. The blossom-dwelling bacterium naturally competes with fire blight for space and nutrients that both need to survive. Unlike its rival, E325 doesn't cause disease, according to Pusey. He has shown that spraying E325 onto blossoms enables the bacterium to crowd out its fire blight rival so the disease is less able to cause harm.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

16. *March 25, Bloomberg* — **Taiwanese government to lift ban on U.S. beef imports next month.** Taiwan will resume U.S. beef imports, 15 months after banning the product because of the first U.S. case of mad cow disease. The island, once the sixth-largest buyer of U.S. beef, will allow imports of boneless meat from cattle younger than 30 months starting on April 16, the island's Department of Health said on its Website. The decision was made after a panel of experts convened by the agency spent months deliberating and evaluating U.S. testing and other safety measures. Australia and New Zealand took over Taiwan's beef import market last year after the ban against U.S., which had a fifth of the island's beef import market before the mad cow case. The disease, formally called bovine spongiform encephalopathy, has a fatal human variant. Taiwan said its U.S. beef must come from slaughter and packing houses registered with the Department of Health and approved by the U.S. Department of Agriculture (USDA). The meat also must be USDA certified.

Source: <http://www.bloomberg.com/apps/news?pid=10000103&sid=aCSNqbG2I6Mk&refer=us>

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

## **Food Sector**

Nothing to report.

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

## **Water Sector**

Nothing to report.

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

## **Public Health Sector**

17. *March 25, Associated Press* — **Outbreak of Marburg virus in northern Angola spreads to capital.** Five cases of a fever that has killed at least 95 people along the Angola-Congo border have been detected in the Angolan capital, according to a news agency report Friday, March 25. The Portuguese news agency Lusa quoted Vita Mvemba, the chief government health official for the province that includes Luanda, Angola, as saying two of the patients -- a 15-year-old boy and an Italian aid worker -- had died. Mvemba said the two had come from Uige, the province along the Congo border where the outbreak was first reported. The agency did not say whether the three other patients had been in Uige. It said those three, one of them a child, were hospitalized in Luanda. The World Health Organization (WHO) said Tuesday, March 22, that the illness was Marburg, a disease similar to Ebola. Analysis had identified 102 cases of the virus since October, 95 of which had proved fatal, WHO said. Angolan officials put the death toll at 98. Doctors have no vaccine or cure for Marburg, which, WHO said, "can be rapidly fatal."

Source: <http://www.freewmexican.com/news/11910.html>

18.

*March 25, Agence France Presse* — **Two new cases of bird flu in Vietnam.** Two more people have tested positive for bird flu in northern Vietnam, including a 17-year-old girl who died, the director of a Hanoi hospital said. The girl, from Nam Dinh province 60 miles south of Hanoi, was taken to hospital on Monday, March 21, and tested positive for the H5N1 virus two days later. A woman of 40 from Quang Ninh province bordering China has also tested positive and has been in hospital since the end of the last week in a stable condition.

Source: [http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=6&u=/afp/20050325/hl\\_afp/healthfluvietnam\\_050325080811](http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=6&u=/afp/20050325/hl_afp/healthfluvietnam_050325080811)

**19. March 24, Associated Press** — **EPA sensors for detecting bioterrorism attack faulted.** Cities are not getting all the protections President Bush ordered last year to detect a biological terrorism attack, the Environmental Protection Agency's (EPA) internal watchdog said Thursday, March 24. The report from EPA Inspector General Nikki L. Tinsley's office said the agency hasn't ensured the reliability, timeliness and efficiency of air sampling that Bush directed be part of a \$129 million early warning system. "The failure of EPA to completely fulfill its responsibilities raises uncertainty about the ability of the BioWatch program to detect a biological attack," Tinsley's report said. Specifically, the report said EPA sometimes placed sensors too far apart, failed to make sure they were all in secure locations and didn't always factor in topography and seasonal wind pattern changes in some cities. President Bush signed an order last April directing agencies to help protect the country from an attack with biological agents. Using up to 50 sensors per city, the network is designed to provide coverage for 80 percent of the population in the cities in which it is used. The intent is to detect a biological agent within 36 hours of release and give authorities time to react properly.

Source: <http://www.signonsandiego.com/news/nation/terror/20050324-1437-biologicalterrorism.html>

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

## **Government Sector**

Nothing to report.

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

## **Emergency Services Sector**

**20. March 25, Sweetwater Reporter (TX)** — **Texas fire department to conduct weapons of mass destruction awareness training.** The Sweetwater Fire Department (SFD) announced it will hold a free Weapons of Mass Destruction (WMD) Awareness Level Training class on March 28–29. The class, which is sponsored by the Department of Homeland Security (DHS), establishes a common baseline to ensure nationwide consistency in WMD education and training, and is open for anyone interested in learning. According to DHS's student manual, the course standardizes the minimum awareness level learning objectives that will be included in all federal, state, and local courses provided through the use of federal funds. It is not intended as a replacement for all existing WMD awareness level courses. The course would include topics ranging from chemical and biological agents, radiological materials and explosive devices and will tackle basic information in dealing with awareness and preparedness. A test

will also be conducted after the classes, and attendees will receive certificates from DHS.

Source: <http://www.sweetwaterreporter.com/articles/2005/03/25/news/news5.txt>

21. *March 25, Associated Press* — **Norfolk plans to be prepared for a tsunami.** Norfolk, VA, could become the first U.S. city along the Atlantic or Gulf coasts to have plans in place to deal with a tsunami. The city is the final stages of applying for designation as a "TsunamiReady" community under a program administered by the National Weather Service. The program is already in wide use on the West Coast and in Alaska. The city's efforts were cited recently at the National Hurricane Conference as emergency planners held a workshop in New Orleans on the threat of tidal waves. Jim Talbot, Norfolk's deputy coordinator of emergency services, says the threat of a tsunami hitting Norfolk is "very, very small," but he says they should prepare. Source: <http://www.wavy.com/Global/story.asp?S=3130294>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

22. *March 24, SecurityTracker* — **Microsoft Windows Remote Desktop 'TSShutdown.exe' remote denial of service vulnerability.** A vulnerability was reported in Microsoft Windows Remote Desktop. A remote authenticated user can shutdown the target system. A non-administrative user can remotely shut down a Microsoft Windows XP Service Pack 1 (SP1)-based computer by using the TSShutdown.exe command. This problem occurs because the Remote Desktop does not check the Force shutdown from a remote system user right. A hotfix is available from Microsoft Product Support Services. See the knowledge base article for more information: <http://support.microsoft.com/kb/889323/>  
Source: <http://www.securitytracker.com/alerts/2005/Mar/1013552.html>
23. *March 24, Associated Press* — **Federal Election Commission officials weigh limited Internet activity rules.** Federal Election Commission (FEC) officials on Thursday, March 24, took their first steps in extending campaign finance controls to political activity on the Internet, asking for public input on limited regulations for the freewheeling medium. Commissioner Ellen Weintraub, who took the lead on drafting proposals with vice chairman Michael Toner, described the steps as "restrained." The commission emphasized a hands-off approach to bloggers, or authors of Web logs, among the loudest and unruliest voices online. The draft guidelines suggest applying limits that exist in other media to certain political advertising on the Web and political spam e-mail. The commission said it was exploring Internet regulation reluctantly – ordered to do so by a court – and with the lightest touch possible, exempting everything except certain kinds of paid political advertising. But the Center for Individual Freedom, a nonprofit advocacy group, said any regulation is too much. FEC Website: <http://www.fec.gov/>  
Source: [http://www.washingtonpost.com/wp-dyn/articles/A63872-2005Mar\\_24.html](http://www.washingtonpost.com/wp-dyn/articles/A63872-2005Mar_24.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 identified a recent increase of reported P2P incidents. P2P file sharing technology provides Internet users with the potential to share local files with a potentially unlimited number of other Internet users. As a result, the usage of P2P software may allow for sensitive data or personal information to be leaked from computer systems. Further, P2P may provide a vector for malicious code to be introduced into an enterprise environment.

#### Current Port Attacks

<b>Top 10 Target Ports</b>	445 (microsoft-ds), 135 (epmap), 53 (domain), 80 (www), 1025 (----), 139 (netbios-ssn), 1026 (----), 1027 (icq), 6346 (gnutella-svc), 1433 (ms-sql-s) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://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. *March 28, Associated Press* — Bomb threats delay professional basketball game.** A bomb threat that delayed the National Basketball Association matchup between the Detroit Pistons and the Indiana Pacers for over an hour Friday, March 25 was one of four received that night regarding the game, police said. The game was delayed after a caller told officials at The Palace, the Detroit Pistons' arena, that there was a bomb in the Pacer's locker room. After the news of the first threat became public a second threat was called in to the Auburn Hills Police communications center. The Palace switchboard also received two more bomb threats at the end of the game, police said. It does not appear the calls were made by the same person, police said, and all the calls are being investigated.

Source: <http://abcnews.go.com/Sports/wireStory?id=616212>

[[Return to top](#)]

## General Sector

**25. *March 28, The Associated Press, Agence France-Press* — Letters warn of French rail bombing.** A shadowy group called AZF that is seeking to extort money through bomb threats against rail lines in France has warned of a new "Madrid tragedy" in letters to the authorities in Paris, according to French officials. The officials added that the threats were not specific and that they spoke of a lesson being taught and set a date for further contact with the authorities in May. The state prosecutor's office said in a statement on Friday, March 25, that the group—or possibly individual—calling itself AZF sent two letters on Thursday, one to President Jacques

Chirac and one to the Interior Ministry. Both of the identical letters, which were posted in France, contained pieces of detonators of the kind that can be used to set off a bomb, according to the officials, who asked not to be identified. AZF first appeared in December 2003 with a promise to blow up rail lines unless it were paid \$5 million, plus an additional \$1 million. A sophisticated bomb was discovered hidden under stones on a train line between Paris and Toulouse underlined the seriousness of the threat. On March 25 last year, one day after another device was found on a rail line, AZF said it had suspended its actions but warned it would be back with a more effective "force of persuasion."

Source: <http://www.iht.com/articles/2005/03/27/news/terror.html>

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

## **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](mailto: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](mailto: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](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original

source material.