Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 06 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 federal investigators are looking into reports that some sections of a southwest Washington railroad track had given trains a rough ride in the days before a four−car passenger train derailed, injuring more than two dozen people. (See item 5)

- The Departments of Homeland Security and State have announced the Western Hemisphere Travel Initiative, which will require all U.S. citizens, Canadians, citizens of the British Overseas Territory of Bermuda, and citizens of Mexico to have a passport or other accepted secure document to enter or re−enter United States by 2008. (See item 6)

- The Hartford Courant reports that on Monday, the first day of TOPOFF 3, an international drill, it became obvious that victims in a Connecticut terrorist attack might face a significant delay before receiving medical treatment. (See item 20)

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 05, The Arizona Republic* — **Bill would authorize "shoot to kill" order at nuclear plant.** The Arizona Legislature on Monday, April 4, sent Governor Janet Napolitano a bill that would authorize private security guards to shoot and kill to protect the Palo Verde nuclear plant, located in Wintersburg, AZ. On a 52−3 vote, the House endorsed Senate Bill 1214, which

would give security guards the authority to shoot those believed to be terrorists or other intruders who threaten the facility. The measure had already cleared the Senate. Supporters say the measure is necessary because the federal government expects armed private guards to use lethal force. The proposed law won't stop peaceful protesters from expressing their views, said George Diaz, a lobbyist for Pinnacle West Capital Corp., the parent company of Arizona Public Service Co., which operates the plant.
Source: http://www.azcentral.com/arizonarepublic/local/articles/0405 nuclear05.html

[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

2. *April 05, Associated Press* — **Social Security numbers on Medicare cards reviewed.** Amid growing concerns about identity theft, the federal government is reviewing its practice of putting Social Security numbers on Medicare cards that go out to about 41 million Americans. Taking off the numbers would represent a major shift in policy for the Centers for Medicare & Medicaid Services (CMS), the agency that administers Medicare and oversees, along with the states, Medicaid. Medicare is the federal health−insurance program for the elderly and disabled, while Medicaid is a program for the poor. "We're considering whether there are other ways to identify people ... but whether we could, and how we would go about changing it for everyone, has not been determined," said Gary Karr, a CMS spokesperson. "There would be a huge systems change that you would have to undertake, and you'd have to figure out what is the cost, and if that cost is worth it." Social Security numbers have been used to identify individuals since the Medicare program was created in 1965. However, critics have urged the federal government to cease printing the numbers on Medicare cards, saying that it puts people at risk for identity theft, especially if their wallets are lost or stolen.
   Source: http://news.yahoo.com/news?tmpl=story&u=/ap/20050405/ap_on_bi_ge/social_security_cards_1

3. *April 05, ZDNet (UK)* — **International bank deluged by viruses.** The British technology police, the National Hi−Tech Crime Unit, said Monday, April 4, that UK companies receive an average of seven viruses a day. "I was interested to hear it was seven attacks a day," said Alan Jebson, International bank HSBC's group chief operating officer. "On our worst day last year, we had 100,000 attacks," said Jebson, speaking at the e−Crime Congress in London. HSBC holds more than a trillion dollars in assets, making it a tempting target for virus writers and hackers. However, e−mail identity theft scams are posing a greater threat to the bank's 18.9

million online customers, Jebson said. "We are naturally very concerned about anything that would damage online banking," Jebson said. "Customers will only do business online if they are convinced it is secure. Customers are no longer sure whether e−mails from financial institutions are genuine," Jebson said. e−Crime Congress: http://www.e−crimecongress.org/ecrime2005/website.asp
Source: http://news.zdnet.com/2100−1009_22−5655520.html

4. *April 04, IDG News Service* — **German bank is hit by phishing attack.** Germany's Postbank has been the target of another phishing attack, its third after two back−to−back assaults last year. "The attack came around midnight, but as far we as know, none of our customers have revealed any confidential banking information," said Postbank spokesperson Hartmut Schlegel on Monday, April 4. Customers of the large state−owned retail bank received an e−mail requesting them to enter two transaction authorization numbers for security reasons. The e−mail address was: security@postbank.de. The Website was blocked "within a relatively short period of time," Schlegel said. He declined to provide details about who blocked the site and how. Until last year, most phishing attacks have been aimed at customers of banks in English−speaking countries, such as the U.S., UK, and Australia, but over the past few months, numerous other countries, including Germany, have become targets. Postbank suffered two attacks last August, following a separate attack on Deutsche Bank AG. All three of the phishing e−mail messages were written in poor German, according to Schlegel. "This raised a warning flag to most of our customers," he said.
Source: http://www.infoworld.com/article/05/04/04/HNpostbank_1.html

[Return to top]

Transportation Sector

5. *April 05, Associated Press* — **Track studied after derailment.** Federal investigators on Monday, April 4, were looking into reports that some sections of a southwest Washington railroad track had given trains a rough ride in the days before a four−car passenger train derailed on Sunday, April 3, injuring more than two dozen people. A federal railroad inspector reported rough riding March 23 on a track about 250 feet from the accident site, National Transportation Safety Board (NTSB) investigator Cy Gura said at a news conference. At the time, Burlington Northern Santa Fe Railway Co. (BNSF), which owns and operates the track, acknowledged receiving the report and said it would respond, but did no other follow−up, Gura said. The track was reopened late Monday afternoon, said Seattle−based BNSF spokesperson Gus Melonas. The derailed cars had been removed, he said. The cause of the derailment "could be anything," Gura said, suggesting there could have been an alignment problem, a warp, or a slight drop in elevation on one side of the tracks. The derailment occurred on the main Columbia River Gorge rail line. About 40 trains use that track daily −− two passenger trains, one in each direction, and dozens of freight. Nine freight trains were rerouted Sunday.
Source: http://www.registerguard.com/news/2005/04/05/d3.amtrakderail .0405.html

6. *April 05, Department of Homeland Security* — **New passport initiative announced.** The Departments of Homeland Security and State announced on Tuesday, April 5, the Western Hemisphere Travel Initiative to secure and expedite travel. The Western Hemisphere Travel Initiative will require all U.S. citizens, Canadians, citizens of the British Overseas Territory of

Bermuda, and citizens of Mexico to have a passport or other accepted secure document to enter or re−enter United States by January 1, 2008. Currently, U.S. citizens, and some citizens of other countries in the Western Hemisphere are not required to present a passport to enter or re−enter the U. S. when traveling within the Western Hemisphere. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA, also known as the 9/11 Intelligence Bill), signed into law on December 17, 2004, mandated that the Secretary of Homeland Security, in consultation with the Secretary of State, develop and implement a plan to require U.S. citizens and foreign nationals to present a passport, or other secure document when entering the United States. For addition information on the Travel Initiative see http://www.dhs.gov/dhspublic/display?content=4434 Also refer to http://www.travel.state.gov.
Source: http://www.dhs.gov/dhspublic/display?content=4433

7. *April 05, Reuters* — **ATA wins court approval for Chicago Express sale.** ATA Holdings, parent of bankrupt ATA Airlines, won approval from a federal bankruptcy judge Monday, April 4, to sell its regional carrier, Chicago Express, to Okun Express. Indianapolis−based ATA, in bankruptcy since October, said last week that it had selected Indianapolis−based Okun as the highest and best bidder for Chicago Express. Exact terms of the sale were undisclosed, but a lawyer for ATA said the total sale price would be between $5.44 million and $6.44 million.
Source: http://www.usatoday.com/travel/flights/2005−04−04−ata−sale_x .htm

8. *April 04, Chicago Sun−Times* — **United looks east to boost bottom line.** United Airlines, struggling to recover financially after more than two years in bankruptcy court, is looking to the economically booming Far East for new profits. In a message to employees on Friday, April 1, United CEO Glenn Tilton said the Elk Grove Village, IL−based company must continue to focus on its role as a global airline, particularly in the Asia Pacific market, where the carrier has almost a quarter of its total capacity. Tilton said opportunities in Asia include both business and leisure travel. "As the middle class and their disposable income continue to grow in Asia, more and more people in this market are traveling to the United States," Tilton said. United is not the only U.S. hub airline that sees profits in the Orient, and competition for the Asian market is heating up. Friday, the Transportation Department awarded American Airlines the right to fly non−stop from Chicago to Shanghai beginning April 2, 2006 −− a route United started flying last October. United and Northwest Airlines are the dominant U.S. carriers in the Asian market.
Source: http://www.suntimes.com/output/business/cst−fin−united04.htm l

9. *March 31, Transportation Security Administration* — **Explosives detection capability for screening checked baggage expanded.** The Transportation Security Administration (TSA) on Thursday, March 31, announced the purchase of eight Reveal Explosives Detection Systems (EDS) for screening checked baggage. The Reveal CT−80 machines are less in cost and smaller than the EDS machines currently in use. “This new equipment is an example of our continuing partnership with the private sector to develop, test and deploy the latest, state−of−the−art technology,” said Rear Adm. David M. Stone, USN (Ret.), Assistant Secretary of Homeland Security for TSA. The machines are to be deployed for operational testing and evaluation at Gulfport−Biloxi (MS) International Airport, Newark, (NJ) Liberty International Airport and John F. Kennedy International Airport (NY) by mid−May 2005 and will supplement Explosives Trace Detection and/or EDS equipment already in place. The selected airports have limited floor space, making them preferable for this pilot program. The field tests will last from 30 to 45 days at each airport and will be used to evaluate the machine’s effectiveness in an airport

environment as well as its impact on security and customer service.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 011293b

[Return to top]

Postal and Shipping Sector

10. *April 05, Missourian* — **Postal service unveils anthrax testing.** The Columbia, MO, mail processing and distribution center will begin using its new Postal Service Biohazard Detection System Tuesday, April 5. The system is designed to detect anthrax by collecting air samples above mail that moves through high−speed equipment. The processing center in Columbia is one of five centers in Missouri to receive the system. The others are in Kansas City, St. Louis, Springfield, and Cape Girardeau. More information about the Biohazard Detection System at http://hqdainet.army.mil/mpsa/nov_conf/ppt/pdf/BDS.pdf
Source: http://columbiamissourian.com/news/story.php?ID=13093

[Return to top]

Agriculture Sector

11. *April 05, Thoroughbred Times* — **Florida officials consider making strangles a reportable disease.** Officials from Florida's Department of Agriculture expect to confirm additional cases of strangles at Palm Meadows Training Center and will consider placing the highly contagious respiratory disease on the state's list of reportable diseases. As a reportable disease, horsemen would be required to notify officials of suspected cases of strangles. Five horses have tested positive at Palm Meadows for strangles. Mike Short, manager of equine programs for the Florida Department of Agriculture, said he expects an unknown number of additional positives.
Source: http://www.thoroughbredtimes.com/todaysnews/newsview.asp?recno=53853&subsec=1

12. *April 05, Waterloo Cedar−Falls Courier (IA)* — **Testing shows no chronic wasting disease in Iowa.** Results from tests completed at the National Veterinary Services Lab in Ames, IA, confirmed that none of the 4,579 Iowa whitetail deer tested for chronic wasting disease (CWD) during the 2004−05 season showed any signs of the disease. Samples were collected from all 99 counties in Iowa; however the majority −− roughly 3,500 −− was taken in the seven Mississippi River border counties stretching from Allamakee County south to Scott County. Emphasis was placed on that area due to the prevalence and proximity of CWD in Wisconsin and Illinois.
Source: http://www.wcfcourier.com/articles/2005/04/05/sports/iowa_outdoors/doc4252a8a7edd4d584201066.txt

[Return to top]

Food Sector

13. *April 05, Wisconsin Daily Rapids Tribune* — **Del Monte improves food security.** Del Monte

Foods in Plover, WI, is increasing its security to prevent bioterrorism from contaminating the nation's food supply. The security features would limit entry to the facility through a monitored fence. A six−foot−tall chain link fence with barbed wire on top will enclose the Plover facility with access regulated by a 30−foot−wide electric gate and guardhouse near the front office building.
Source: http://www.wisinfo.com/dailytribune/wrdtlocal/28554320259737 8.shtml

14. *April 04, Ohio State University Extension* — **Ohio State University Extension joins national food safety network.** Veterinary researchers with Ohio State University Extension and the Ohio Agricultural Research and Development Center (OARDC) have joined a team of food−safety experts awarded five million dollars by the U.S. Department of Agriculture (USDA) to study the most common causes of food−related illnesses and act as a response team to help control major outbreaks. The Food Safety Research and Response Network includes experts from 18 U.S. and Canadian institutions. The team will conduct research on E. coli, salmonella, campylobacter, and intestinal viruses. "This project will help improve food safety for years to come by bringing together the nation's leading experts in pre−harvest food safety," said Colien Hefferan, USDA's Cooperative State Research, Education, and Extension Service administrator. "Several pathogens will be studied to determine where they are found in the environment, how are they sustained and how they infect herds. With this team approach, researchers with a broad range of expertise are working together to tackle persistent and challenging problems." The Food Safety Research and Response Network will also serve as a response team that can be mobilized to conduct focused research to control major episodes of food−related illnesses. These episodes could include investigation of health problems associated with agricultural bioterrorism and the deliberate contamination of agricultural commodities.
Source: http://extension.osu.edu/~news/story.php?id=3086

[Return to top]

Water Sector

15. *April 04, North County Times (CA)* — **California sewage spill linked to vandalism.** A portion of Carlsbad State Beach in Carlsbad, CA, was closed Monday, April 4, after a sewage spill over on Saturday, April 2, in south Vista, officials said. The spill, which Vista city officials determined was caused by vandalism to a sewer manhole, flowed into the Agua Hedionda Creek and into the Agua Hedionda Lagoon and then to the Carlsbad beach. The 28,600−gallon spill forced the closure of the beach 300 feet both north and south of the lagoon outlet, said Clay Clifton, the Ocean and Bay Recreation Water Program coordinator for the San Diego County Department of Environmental Health (DEH). The DEH estimated that the spill lasted about an hour and a half on Saturday morning. In addition to posting closures at beaches, DEH has posted signs warning of sewage contaminated water at access points to the Agua Hedionda Creek within Buena Vista Park in Carlsbad.
Source: http://www.nctimes.com/articles/2005/04/05/news/coastal/4405 195040.txt

[Return to top]

Public Health Sector

16. *April 05, Reuters* — **Bird flu strain detected in North Korea.** The H7 strain of bird flu, previously undetected in Asia, has been found in North Korea, which has culled thousands of chickens to contain its first such outbreak, a top UN expert said on Tuesday, April 5. "We have a new situation because H7 has so far not occurred in Asia," said Hans Wagner, a senior official with the UN Food and Agriculture Organization. Apart from H5N1, H7 is one of two other avian strains which can cause illness in humans, but the outbreaks were not as severe as those caused by the H5N1 strain.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=8084836

17. *April 05, Agence France Presse* — **Marburg virus toll in Angola hits 155, fear intensifies in Luanda.** An outbreak of the Marburg virus has intensified in Angola, claiming more than 29 lives over the past four days and taking the nationwide toll to 155, heightening fear of the disease in the capital Luanda, authorities said Monday, April 4. Angolan health minister Sebastiao Veloso said the toll climbed to "175 cases, among them 155 dead, all from the province of Uige," the epicenter of the outbreak in the country's north on the border with the Democratic Republic of Congo. In Luanda, international experts were working round−the−clock to complete a special isolation ward to treat incoming cases from around the country. The Angolan health ministry said the unit would not be ready for at least the next five days.
Source: http://www.reliefweb.int/rw/RWB.NSF/db900SID/RMOI−6B62NB?Ope nDocument

18. *April 05, Reuters* — **Two suspected cases of bird flu in Vietnam.** Two more Vietnamese, a 12−year−old girl and a woman, are in hospital with suspected bird flu, the official Vietnam News Agency said on Tuesday, April 5. The girl, who lives near a poultry slaughterhouse, was in an isolation ward on Monday, April 4, in the northern city of Haiphong, the head of the city's Health Department was quoted as saying. The woman was taken to hospital in Hue the previous day and both were being tested to see if they had contracted the H5N1 virus which has killed 49 people in Asia. The Tien Phong newspaper said researchers at the National Institute for Hygiene and Epidemiology meanwhile were trying to find what had caused the acute pneumonia which killed a 34−year−old doctor in the northern province of Quang Ninh. He fell sick on Friday, April 1, his breathing worsened quickly despite emergency treatment for Severe Acute Respiratory Syndrome, and he died on Sunday, April 3, the newspaper said.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=8084714

19. *April 05, Agence France Presse* — **Twenty−seven patients hit by superbug.** An antibiotic−resistant strain of bacteria has been detected in another 27 patients at one of Singapore's largest hospitals, bringing the total number of diagnosed cases to 42, health officials said. Of the 42 patients hit by the vancomycin−resistant enterococci (VRE) bacteria, only one is an infected patient while the rest are carriers, the Singapore General Hospital said Monday, April 4. The hospital first reported last Friday 15 patients were diagnosed with the bacteria and saw a cluster of six VRE cases last year. More information about VRE is available at http://www.cdc.gov/ncidod/hip/ARESIST/vre.htm
Source: http://dailytelegraph.news.com.au/story.jsp?sectionid=1274&s toryid=2918423

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

20. *April 05, Hartford Courant (CT)* — **Delays in medical treatment found during drill.** On Monday, April 4, the first day of TOPOFF 3, an international drill, it became obvious that victims in a Connecticut terrorist attack might face a significant delay before receiving medical treatment. In the exercise designed to reveal weaknesses in emergency response, the most obvious problem seemed to be a shortage of ambulances for the field of burned and bloodied "victims" on New London, CT's waterfront. The final report that will detail the weaknesses in the state's response is months away. But for the rest of this week, Connecticut officials will be among 10,000 people in three countries working their way through the largest terrorism drill in U.S. history. After the special−effects boom of a terrorist car bomb −− which events would suggest was a violent distraction from an earlier release of deadly chemicals −− volunteer role−players took their places. TOPOFF 3, the third in a congressionally mandated series of drills that started before 9/11 in 2000, was designed to teach hard lessons like that. The $16 million exercise joined hundreds of agencies in the United States, United Kingdom and Canada for a complex series of mock events culminating in the chemical attack at New London and a simultaneous biological attack in New Jersey.
Source: http://www.courant.com/news/local/hc−topoff0405.artapr05,0,7376909.story?coll=hc−big−headlines−breaking

21. *April 04, Federal Computer Week* — **Web−based tool will aid emergency and public safety efforts.** Operation Archangel, a Web−based system developed by the city and county of Los Angeles to aid emergency workers, is set to be deployed this summer. The system identifies sites that are vulnerable to terrorist attacks and coordinates information about them. The heart of the Archangel system is a secure online database called the Automated Critical Asset Management System. It stores site assessment data and gathers information from external databases. It works with mapping systems and aggregates relevant information. Incident commanders, first responders and other authorized employees can access the system to view lists of critical assets and plans for enhancing security, protecting buffer zones and responding to emergencies. “If an intelligence analyst tells us that al Qaeda is focused on red buildings, the system can then go through all of the information and come back and say: ‘You have six red buildings. Here’s their level of criticality and vulnerability, here’s their current status, and this is what can be done to increase protection,’” said Lt. Tom McDonald, an officer with the Los Angeles Police Department and a member of the Archangel development team.
Source: http://www.fcw.com/article88474−04−04−05−Print

22. *April 04, InformationWeek* — **New system will let emergency first−responders transmit and receive text, images, and video.** In the next 90 days, the city of Fresno, CA, will begin deploying a new data−communications system to link police, fire, ambulance, and other emergency first−responders via the Web. Like most police departments, Fresno already has a

data−communications system in place. But the current 800−MHz system from Dataradio Inc. lacks encryption capability and is too slow to handle new data types like video, says Pat Rhames, a captain at the Fresno Police Department. "We're interested in adding a system that has more throughput capacity that will take care of what we currently cannot do," he says. The system will use 900−MHz radio technology and transmission towers to allow police officers and headquarters to send and receive text, images, and video via "in−vehicle" computers and handheld PDAs. These capabilities are particularly useful when downloading mug shots and live streaming video of suspects in developing police situations, Rhames says. It also will let officers transmit crime−scene images back to headquarters, access law−enforcement databases, and file police reports.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=C2WDXJ1F433YMQSNDBCCKH0CJUMEKJVN?articleID=160403766

[Return to top]

Information Technology and Telecommunications Sector

23. *April 05, Associated Press* — **Google incorporates satellite maps.** Online search engine Google has unveiled a new feature that will enable its users to zoom in on homes and businesses using satellite images, an advance that may raise privacy concerns. The satellite technology, which Google began offering on Monday, April 4, at http://maps.google.com is part of the package that the company acquired when it bought digital map maker Keyhole. This marks the first time that Google has offered free access to Keyhole's high−tech maps through its search engine. The satellite maps could unnerve some people because the Keyhole technology is designed to provide close−up perspective of specific addresses. There is little reason for people to be paranoid about the satellite maps because the images generally are six to 12 months old, said John Hanke, Keyhole's general manager. “And it's not like you are going to be able to read a license plate on a car or see what an individual was doing when a particular image was taken,” he said. Google's free satellite maps initially will be limited to North America, with images covering roughly half the United States, Hanke said.
Source: http://www.nytimes.com/aponline/technology/AP−Google−Maps.ht ml?

24. *April 04, FrSIRT Advisory* — **Mozilla Firefox/Suite information disclosure vulnerability.** A new vulnerability was identified in Mozilla Firefox/Suite, which may be exploited by attackers to disclose sensitive information. The browser's javascript implementation does not properly parse lamba list regular expressions. This flaw is due to an error in the JavaScript engine, which may be exploited by attackers to disclose arbitrary heap memory regions. There is no solution at this time.
Source: http://www.frsirt.com/english/advisories/2005/0312

25. *April 04, CNET News* — **Florida files multimillion−dollar spam suits.** The Florida Attorney General's office has filed its first claims under the state's antispam law, charging two men with masterminding a scheme that marketed fraudulent online businesses via e−mail. Florida Attorney General Charlie Crist charged two Tampa residents accused of running an operation that generated over 65,000 deceptive e−mails since 2003, including 48,000 messages sent after the Florida Electronic Mail Communications Act took effect on July 1, 2004. The defendants face up to $24 million in fines. Like the federal Can−Spam Act, the Florida law prohibits the

distribution of unsolicited commercial e−mail that contains false or deceptive subject information, or that is sent from invalid e−mail addresses. Under the law, violators face a penalty of up to $500 for every illegal e−mail message they send to Florida residents. "Spam is a pervasive and growing threat to unsuspecting computer users everywhere," Crist said in a statement. "The spam itself is illegal, but it is made even worse when it seeks to rip off Florida consumers. Florida's antispam law was adopted precisely to stop operations such as this one."
Source: http://news.com.com/Florida+files+multimillion−dollar+spam+suits/2100−1030_3−5653662.html

26. *April 04, eWeek* — **Cyber−terrorism analyst warns against complacency.** Cyber−security and counterterrorism analyst Roger Cressey on Monday, April 4, pleaded with IT executives not to underestimate the threat of "national cyber−event" targeting critical infrastructure in the United States. During a keynote address at the InfoSec World 2005 conference, Cressey warned against discounting the danger of the Internet being used in a terrorist−related attack. "It may not be a terrorist attack, but a cyber−event is a very, very serious possibility. When it happens, it will have serious economic impact on our critical infrastructure." Cressey, who served as chief of staff to the president's Critical Infrastructure Protection Board at the White House, said there was enough evidence that U.S. enemies were actively using the Web to recruit, organize and communicate terrorism activities. Cressey, the on−air counterterrorism analyst for NBC News, said the rapid rate in which Internet security vulnerabilities was being detected only adds to the worry. Cressey used part of his keynote to call on VoIP (Voice over Internet Protocol) developers to put security on the front burner. Describing VoIP security as the great challenge of this decade, he said it would be a "big mistake" for another nascent industry to emerge without built−in protections.
Source: http://www.eweek.com/article2/0,1759,1782286,00.asp

27. *April 04, internetnews.com* — **Report: VoIP subscribers to grow to 27 million by the end of the decade.** In 2005, research firm IDC expects that three million Americans will subscribe to residential VoIP (Voice over Internet Protocol) services. By 2009, the number of subscribers is forecast to balloon to 27 million. IDC notes that even though the VoIP market is already crowded with next−generation carriers like Vonage, as well as traditional carriers like AT&T, cable vendors will enter the fray in 2005 further cluttering the VoIP service market. According to IDC, VoIP still has a long way to go before it achieves critical mass in comparison to the existing time−division multiplexing (TDM)−based services. VoIP services have recently been the subject of discussion on Capitol Hill. One of the downside issues concerns 911 services (or lack thereof) provided by VoIP carriers. Report information:
http://www.idc.com/getdoc.jsp?containerId=prUS00106805
Source: http://www.internetnews.com/stats/article.php/3495076

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 reports two denial of service (DoS) issues identified in the AutoProtect functionality of the Symantec Norton AntiVirus consumer product, where a real time scan of a specific file type can cause a system crash, Blue Screen of Death (BSOD), with both Symantec Norton AntiVirus 2004 and 2005 Windows applications. This type of file, while not malicious on it's own, could be maliciously introduced either remotely from outside the system through email or over http, or internally by an authorized user to disrupt service on a targeted system.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 28755 (−−−), 135 (epmap), 11965 (−−−), 139 (netbios−ssn), 4010 (samsung−unidex), 1026 (−−−), 1027 (icq), 80 (www), 1025 (−−−) 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

28. *April 05, Knight Ridder News* — **Italian security worries rise as millions mourn.** With two million pilgrims and 200 world leaders descending on the city in advance of the papal funeral on Friday, April 8, Rome is grappling with a logistics and security challenge that officials there −− or anywhere −− have rarely seen. The most recent two papal funerals, both in 1978, attracted a mere 750,000 and 500,000 mourners, respectively, and just a few heads of state. But Friday's farewell to John Paul II is expected to draw several times those numbers, including President George W. Bush, who will be the first U.S. president to attend a papal funeral mass. That has sent Italian officials into an around−the−clock scramble to plan for both mundane and special needs, from security to thwart any terrorist attack to providing food, shelter and medical care to a number of visitors that may almost equal the city's 2.5 million population. "For us, it will be an extraordinary challenge," Rome Mayor Walter Veltroni said Sunday, April 3. Michele Calderone, a spokesperson for Italy's Interior Ministry, declined to discuss what security precautions would be taken to ensure the safety of the tens of thousands expected to jam into St. Peter's Square to be near the papal funeral service.
Source: http://www.freep.com/news/religion/secure5e_20050405.htm

29. *March 30, Government Accountability Office* — **GAO−05−269: September 11: Recent Estimates of Fiscal Impact of 2001 Terrorist Attack on New York (Report).** In 2002, the

Government Accountability Office (GAO) reported that the New York budget offices estimated that from the terrorist attack, New York City sustained tax revenue losses of $1.6 billion for 2002 and $1.4 billion for 2003, New York State $1.6 billion for 2002 and $4.2 billion for 2003. GAO found some limitations to these estimates, such as that it is likely that they included some of the economic recession under way in September 2001, as well as events after the attack, such as economic fallout from the Enron collapse and accounting firm improprieties. After GAO issued its report in 2002, some New York agencies used revised economic data to assess the attack’s fiscal impact. In this context, GAO was asked to update its report to ascertain whether the recent government studies using revised economic data would provide more precise information on the fiscal impact of the terrorist attack. In doing this work, GAO did not independently estimate the attack’s impact on New York tax revenues. GAO makes no recommendations in this report. In commenting on a draft of this report, the three New York agencies generally agreed with the information presented. Highlights:
http://www.gao.gov/highlights/d05269high.pdf
Source: http://www.gao.gov/new.items/d05269.pdf

[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

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.