Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 01 April 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- Data broker Choicepoint will develop a system that would allow people to review their personal information that is sold to law enforcement agencies, employers, landlords and businesses, the Associated Press reported Wednesday. (See item 5)

- The Associated Press reports that eleven men suspected of illegally entering the United States were arrested this week while aboard a Southwest Airlines flight at the Raleigh−Durham International Airport. (See item 11)

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 31, Associated Press* — **Norway officials predict continued high oil prices.** Oil prices are likely to remain high, and there is nothing Norway can do to increase supplies because the nation's offshore fields are already producing at full capacity, oil minister Thorhild Widvey said Thursday, March 31. Oil prices have been above $50 a barrel, near record levels, and the International Energy Agency has said demand for energy is expected to increase by 60 percent by 2030, pushed up by increasing consumption in places like China and India. "Energy is going to become more and more important on the international agenda," said Widvey. Increased supplies could cool off oil prices, although Widvey said Norway's offshore fields are already at full capacity of about 3.2 million barrels of oil per day plus natural gas. Norway, the world's

third−largest oil exporter after Saudi Arabia and Russia, has remained outside the Organization of Petroleum Exporting Countries (OPEC), which Widvey said would have to provide any extra oil. "There are not many non−OPEC countries with extra capacity. The extra capacity is within OPEC," she said. Widvey said Norway is seeking to maintain current oil production levels for the next few years, but that flows will decline after that.
Source: http://www.washingtonpost.com/wp−dyn/articles/A15217−2005Mar 31.html

2. *March 31, North Adams Transcript (MA)* — **Reward offered for information on destruction of transformers.** Central Vermont Public Service Corp. (CVPS) is offering a $500 reward for information related to the shooting and destruction of two transformers owned by the company. Line crews discovered the transformer shooting after they were called out for the resulting power outage. Replacement of the transformers will cost a total of $8,000. According to Costello, a report of a customer without service on Maple Grove Road in Pownal, VT, came in at approximately 8:30 p.m. on Friday, March 25. The customer reported a loud bang that occurred just before the power outage. Ten minutes later a second call was received reporting another customer nearby without power. "Both transformers were servicing only one or two customers," said Steve Costello, director of public affairs for CVPS. Line crews were dispatched to investigate the outages. Upon arriving at each location, the transformer was found shot and destroyed. “This type of incident is not only costly, but dangerous," Costello said. Transformers are the trash−barrel shaped canisters at the top of telephone poles. They dampen the electrical voltage output to the houses they service.
Source: http://www.thetranscript.com/Stories/0,1413,103~9054~2791756 ,00.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *March 30, KOCO (OK)* — **Oklahoma mall evacuated after chemical scare.** Fire and hazardous materials crews evacuated Crossroads Mall in Oklahoma City, OK, on Wednesday, March 30, after a chemical scare involving the mall's ventilation system. Crews evacuated shoppers and employees after it was discovered that an exterior cleaning solution, not intended for indoor use, was used to clean a department store's air conditioning system. Patrons and staff across the mall were exposed to fumes from the chemical; however, no serious injuries were reported, fire officials said.
Source: http://www.channeloklahoma.com/news/4332348/detail.html

[Return to top]

Defense Industrial Base Sector

4. *March 31, Government Accountability Office* — **GAO−05−301: Defense Acquisitions: Assessments of Selected Major Weapon Programs.** The Department of Defense (DoD) is embarking on a number of efforts to enhance warfighting and the way the department conducts business. Major investments are being made to develop improved weapon systems to combat various threats to U.S. security. While the weapons that DoD ultimately develops have no rival in superiority, weapon systems acquisition remains a long−standing high−risk area.

Government Accountability Office’s (GAO) reviews over the past 30 years have found consistent problems with weapon acquisitions such as cost increases, schedule delays, and performance shortfalls. In addition, DoD faces several budgetary challenges that underscore the need to deliver its new major weapon programs within estimated costs and to obtain the most from those investments. DoD can help resolve these problems by using a more knowledge−based approach for developing new weapons. This report provides congressional and DoD decision makers with an independent, knowledge−based assessment of selected defense programs that identifies potential risks and needed actions when a program’s projected attainment of knowledge diverges from the best practice. It can also highlight those programs that employ practices worthy of emulation by other programs. GAO plans to update and issue this report annually. Highlights: http://www.gao.gov/highlights/d05301high.pdf
Source: http://www.gao.gov/new.items/d05301.pdf

[Return to top]

Banking and Finance Sector

5. *March 31, Associated Press* — **ChoicePoint to allow people access.** An executive of embattled data broker ChoicePoint Inc. said the company is developing a system that would allow people to review their personal information that is sold to law enforcement agencies, employers, landlords and businesses. “You will receive the reports that we have on you,” Don McGuffey, the firm's vice president for data acquisition, told California's Senate Banking, Finance and Insurance Committee on Wednesday, March 30. ChoicePoint's announcement comes a month after it disclosed that thieves used previously stolen identities to create what appeared to be legitimate businesses seeking personal records. As part of safeguards to prevent recurrences, ChoicePoint is altering records to keep clients from having access to complete Social Security and driver's license numbers, McGuffey said. The measures appear to partly satisfy the demands of committee chairwoman Senator Jackie Speier, D−Hillsborough, who has introduced legislation to limit what she said was an industry “that has grown up overnight with no regulations whatsoever.”
Source: http://www.nytimes.com/aponline/business/AP−ChoicePoint−Safe guards.html

6. *March 31, Reuters* — **Software giant targets phishing schemes.** Microsoft Corp. on Thursday, March 31, said it was filing 117 lawsuits against unknown Internet site operators it charged were engaged in phishing schemes to obtain personal and financial information from unsuspecting consumers. The world's biggest software company said it was filing "John Doe" defendant lawsuits in U.S. District Court in Washington state in an attempt to establish connections between worldwide phishers and discover the largest−volume operators. Some scams are getting more and more sophisticated, some by including what looks like a legitimate Internet address link but once clicked on by the user, they are instead directed to a different, fraudulent site asking for personal information.
Source: http://www.cnn.com/2005/TECH/internet/03/31/microsoft.phishi ng.reut/

7. *March 31, Financial Services Sector Coordinating Council* — **Group calls for regional coalitions to provide local support for financial firms' resilience.** The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), a network of financial trade associations and private firms representing thousands of

financial services organizations, on Thursday, March 31, called for a strong regional strategy to coordinate local responses to a crisis or business disruption. FSSCC's Statement on Regional Infrastructure Protection Coalitions is intended to guide financial firms located together to organize their responses not only to potential national disruptions to financial services, such as terrorism, natural disasters or cyber attacks, but also to local incidents affecting the sector's resilience. The new regional strategy makes specific mention of the ChicagoFIRST model as an example of how a sector can organize itself to respond to local incidents and issues. ChicagoFIRST was formed in 2003 for the express purpose of building a close operational relationship between private institutions and public agencies in a specific geographic area, in order to better protect the critical infrastructure of the financial services sector in that locality. Statement on Regional Infrastructure Protection Coalitions: http://www.fsscc.org/reports/Statement_on_Regional_Coalition s.pdf. ChicagoFIRST: https://chicagofirst.org/
Source: http://www.fsscc.org/news/2005_coalitions.html

8. *March 30, MosNews (Russia)* — **Hackers steal Russian Central Bank transactions.** Russian hackers have stolen the database of Central Bank transactions from April 2003 to September 2004, the Vedomosti newspaper reported on Wednesday, March 30. In February, an advertisement appeared on the Internet offering copies of the Russian Central Bank database detailing transactions over a period of 18 months. The database was offered for $800−1000, according to one of those selling the information, the paper said. A month ago, the database was selling at $1500−2000. Executive secretary of the Moscow government's Business Council Information Market Security Commission, Oleg Yashin, said there were several people selling the databases. The transactions database is 60 gigabytes and is sold with a hard disk. Advertisements say the database has detailed information on transactions: payers, addressees, banks and the payment purpose.
Source: http://www.mosnews.com/news/2005/03/30/stolentransactions.sh tml

9. *March 30, Associated Press* — **Federal regulators concerned over money service exclusions.** Federal regulators expressed concerns Wednesday, March 30, over some check cashers, money transmitters and others being excluded from banking services and said they hope to soon issue provisions to address the problem. Some banks are closing the accounts of some of these "money−services" businesses out of fear they might run afoul of regulations aimed at catching money−launderers and terrorist financiers. Banks as well as money−services businesses have asked federal regulators for help. "Money−services businesses are losing access to banking services as a result of concerns about regulatory scrutiny, the risks presented by money−services business accounts and the costs and burdens associated with maintaining such accounts," the banking authorities acknowledged in a joint statement. The statement was issued by the Federal Reserve, Federal Deposit Insurance Corp., the Financial Crimes Enforcement Network, the Office of the Comptroller of the Currency, the Office of Thrift Supervision and the National Credit Union Administration. Regulatory guidance will be issued shortly to address the problem, the statement said. "It is critical that the money−services business industry remain within the formal financial sector and not be driven underground," said Stuart Levey, the Department of Treasury's undersecretary for terrorism and financial intelligence. Joint statement: http://www.fincen.gov/bsamsbrevisedstatement.pdf
Source: http://www.washingtonpost.com/wp−dyn/articles/A13961−2005Mar 30.html

[Return to top]

Transportation Sector

10. *March 31, Associated Press* — **European Union needs more time for biometric passports.** The European Union (EU) on Wednesday, March 30, told the U.S. Congress the bloc needed another year to implement new U.S. rules on secure biometric passports, which include a computer chip with data such as a digital photo of the passport holder. EU justice and interior ministers had said last year they would meet this year's October 26 deadline. But only six of the 25 EU countries – Belgium, Finland, Luxembourg, Germany, Austria, and Sweden – will be ready to issue biometric passports by that date. After October 26, citizens from 27 visa−exempt countries will have to apply for a visa or have a biometric passport. So−called biometric features can reduce patterns of fingerprints, irises, voices and faces to mathematical algorithms that can be stored on a chip or machine−readable strip. EU countries also want to include a fingerprint on the chip. All new U.S. passports issued by the end of 2005 are expected to have a chip containing the holders' name, birth date and issuing office, as well as a photo of the holders' face. The photo is the international standard for biometrics, but countries are free to add other biometrics, such as fingerprints, for greater accuracy.
Source: http://www.nytimes.com/aponline/technology/AP−EU−US−Biometric−Passports.html?

11. *March 31, Associated Press* — **Men suspected of illegally entering U.S. arrested at North Carolina airport.** Eleven men suspected of illegally entering the United States were arrested this week while aboard a Southwest Airlines flight at the Raleigh−Durham International Airport. The men had boarded their flight Tuesday, March 29, by showing federal agents one form of identification – a Mexican voter registration card that contained a name, age and photo, said Thomas O'Connell, resident agent in charge of U.S. Immigration and Customs Enforcement in Raleigh, NC. The men's arrest began when an air marshal on a flight from Las Vegas to Chicago overheard the men discussing how they were smuggled into the United States, O'Connell said. When the flight landed in Chicago, the air marshal called a customs agent who then notified O'Connell's office. In Chicago, the men boarded a second flight to Raleigh. The men had each paid a smuggler $1,000 to cross the border near Douglas, AZ, on or about March 22, O'Connell said. It was not clear how the airline tickets were purchased or how the group got past federal security agents without a passport and using a foreign voter registration card. The men told immigration agents they had come to North Carolina for employment.
Source: http://www.ledger−enquirer.com/mld/ledgerenquirer/news/local /11276413.htm

12. *March 31, Associated Press* — **Atlanta airport latest to use new exit process for foreign visitors.** Hartsfield−Jackson Atlanta International Airport is the latest of 15 U.S. international airports and seaports that are participating in the US−VISIT project. The Atlanta airport started fingerprinting exiting foreigners on Wednesday, March 30. Other airports have been using the system since January 2004. The new exit procedure was needed because although the government collected similar data on foreigners who entered the United States, there was no quick data on when they left the country, said Robert Mocny, deputy director of the US−VISIT program. The US−VISIT program was unveiled as one of the methods of keeping track of foreigners who enter the United States in the post−September 11, 2001 terrorist attack era. The

government has hailed the first phase of the program – photographing and fingerprinting foreign visitors – as a success, as it has kept more than 500 suspected criminals and immigration violators from entering the U.S., Mocny said. Officials hope to be able to put the new exit procedures in place at more international airports and seaports by the end of the year.
US−VISIT Website: http://www.dhs.gov/us−visit
Source: http://www.accessnorthga.com/news/ap_newfullstory.asp?ID=581 95

13. *March 30, GovExec* — **FAA debuts online "human factors" training.** The Federal Aviation Administration (FAA) Tuesday, March 29, announced the debut of an online training program on the importance of "human factors." The Web Course consists of 10 self−guided lessons about the role that sensory, mental and physical capabilities and limitations should play in the design and development of machines. "Improvements to aviation safety and capacity are dependent on developing a national aviation system that is not only technically sophisticated, but also human performance−based and human−centered," Joan Bauerlein, FAA's aviation research and development director, said in a statement. The Web course is designed for people who support FAA system acquisitions, but it is open to the public. FAA employees can receive a training certificate for successful completion. Knowledge of human factors, the agency said, is resulting in aircraft that are safer and easier to fly, and air traffic control systems that are quicker with decision support and more resistant to errors. Web course:
http://www.hf.faa.gov/Webtraining/
Source: http://www.govexec.com/dailyfed/0305/033005b1.htm

[Return to top]

Postal and Shipping Sector

14. *March 30, Associated Press* — **Pennsylvania lawmaker charged in white powder hoax.** A legislator was charged Wednesday, March 30, with lying about a white powder he claimed was inside a letter mailed from a critical constituent. Pennsylvania State Rep. Jeffrey Habay, who is awaiting trial on ethics charges in an unrelated case, claimed he got the letter at home in May and that it had a suspicious white substance inside, raising fears of possible anthrax contamination. The U.S. Postal Inspection Service said the substance was harmless. Habay, a lawmaker from Allegheny County elected to a sixth term in November, faces 20 new counts as a result of the latest complaint, including a felony charge of possessing or using a "facsimile weapon of mass destruction."
Source: http://www.phillyburbs.com/pb−dyn/news/1−03302005−470006.htm l

15. *March 30, Associated Press* — **New anthrax detection system unveiled.** Wyoming's main postal facility unveiled its new biohazard detection system on Tuesday, March 29. The equipment, which checks for anthrax, is targeted for installation in 283 of the largest mail centers across the nation during the next two years. The Cheyenne Mail Processing and Distribution Center is the largest postal facility in the state and handles most of Wyoming's mail. The new Cheyenne system will differentiate between anthrax and other powders by collecting samples of air as mail moves through the machines. Kirkpatrick said the Postal Service has worked closely with the state Health Department, state Department of Homeland Security and Cheyenne's police and fire departments to develop an emergency management plan in case anthrax is detected.

Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2005/03/30/build/wyoming/40−anthrax.inc

16. *March 30, Duluth News Tribune (MN)* — **Machines to ensure mail free from anthrax.** New equipment that will be operational by April 8 should ensure that all letters passing through the mail−processing center in Duluth, MN, are free of anthrax spores. Two sophisticated machines destined will scan envelopes for anthrax. The equipment is part of what the U.S. Postal Service calls its Biohazard Detection System (BDS)−−a collection of technology that automatically collects air samples from mail and analyzes DNA to screen for anthrax.
Source: http://www.duluthsuperior.com/mld/duluthsuperior/business/11 264858.htm

17. *March 30, Associated Press* — **North Dakota postal officials investigate powdery substance linked to drugs .** A suspicious powder that leaked from an envelope at a post office in Jamestown, ND, on Tuesday, March 29, was found to be drugs, authorities said. The post offices in Bismarck, Fargo and Jamestown were closed for about 2.5 hours until tests showed the white powder was a controlled substance, Jamestown Police Chief Dave Donegan said Wednesday. The chief said mail in Jamestown is trucked to and from Bismarck and Fargo, leading those two facilities to close until it was determined the powder was harmless. Further testing is being conducted at the state lab, he said. Postal officials said bulk mail distributed out of Fargo might be a day late because of the shutdown, though first−class mail should be delivered on schedule.
Source: http://www.grandforks.com/mld/grandforks/11269950.htm

[Return to top]

Agriculture Sector

18. *March 31, Reuters* — **Chronic wasting disease found in New York deer.** The first case of chronic wasting disease (CWD) outside the U.S. Midwest or Rocky Mountain region was confirmed in a white−tailed deer in New York State, the state's agriculture department said on Thursday, March 31. The New York Agriculture Department said the animal that tested positive for CWD was a 6−year−old white−tailed doe that was slaughtered from a captive herd in Oneida County. The disease has been found in a dozen U.S. states in the Midwest and Rocky Mountains. New York officials said they quarantined the herd where the infected deer was found, and would kill the remaining animals to test their brains for the disease. The state also quarantined other herds associated with the infected animal.
Source: http://www.reuters.com/newsArticle.jhtml?type=domesticNews&s toryID=8051993

19. *March 31, Agricultural Research Service* — **Major wheat pathogen chosen for genome sequencing.** Agricultural Research Service (ARS) scientists and a cooperator from The Netherlands are leading a project to sequence the genome of a key wheat pathogen. The U.S. Department of Energy's Joint Genome Institute has chosen Mycosphaerella graminicola −− one of the top five wheat disease pathogens −− for genome sequencing. M. graminicola causes major wheat damage worldwide and costs American wheat farmers $275 million a year in yield losses. The cost of fungicide sprays against M. graminicola in Europe is more than $800 million a year. If left unchecked, the fungus causes lesions in wheat leaves that interfere with plant

growth and grain formation. M. graminicola belongs to a family of fungi that cause similar leaf−spotting diseases in bananas, citrus, strawberries, cereal crops, and many other plants. Some of these fungi −− but not M. graminicola −− produce toxins that increase their ability to infect plants. The effect of these toxins on people and animals is not known. The mapping of M. graminicola genes can help researchers understand how the fungus infects crops. This information should help in controlling the fungus and related species.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

20. *March 31, Southeast Farm Press* — **Georgia will monitor soybean rust plots.** University of Georgia (UGA) farm experts will soon begin planting soybean plots throughout Georgia to act as early detectors for an aggressive crop disease first reported across the Southeast last fall. Asian Soybean Rust was reported in the U.S. in November. Tropical storms in September are believed to have picked up spores in South America and delivered them to the Southeastern states. It was first reported in soybean research plots in Louisiana. Later, it was identified in farm fields in Alabama, Arkansas, Florida, Georgia, Mississippi, Missouri, South Carolina, and Tennessee. The UGA Extension Service will monitor 15 to 20 plots on research stations and farms across Georgia, says Phil Jost, a Extension agronomist.
Source: http://southeastfarmpress.com/news/033105−Georgia−rust/

21. *March 25, Nebraska Department of Agriculture* — **Nebraska Department of Agriculture announces emergency information meetings for agricultural producers.** The Nebraska Department of Agriculture (NDA), working with local extension educators, county emergency managers, and the state's veterinarians, will host more than 70 agriculture emergency information meetings for producers at locations across the state, beginning in April and running through the fall. The meetings are intended to educate producers about local and state efforts as they relate to agricultural emergency planning. "In a state that is home to more than 48,000 farms and ranches, advance planning and information is essential to protect the safety of our food supply and our industry," says NDA Director Merlyn Carlson.
Source: http://www.agr.state.ne.us/newsrel/adm/03county_meetings.htm

[Return to top]

Food Sector

22. *March 30, Minnesota Department of Agriculture* — **Alert about potentially contaminated sesame seed paste issued.** The Minnesota Department of Agriculture (MDA) is advising consumers to avoid eating “Ziyad” brand plain tahini after routine testing found the food product to be contaminated with Salmonella bacteria. Tahini is a Middle Eastern sesame seed paste found in specialty stores and major grocery store chains. Based on information gathered by MDA, the product in question is labeled as being of U.S. origin but was actually imported by Ziyad Brothers Importing, of Cicero, IL. The MDA has shared its findings with the U.S. Food and Drug Administration and Illinois state health officials. The contaminated product came from a store in Rochester, MN, but MDA believes the product line has a statewide distribution. MDA has requested that stores remove this product from sale.
Source: http://www.mda.state.mn.us/newsreleases/2005news/05mar30a.ht m

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

23. *March 31, Associated Press* — **Whooping cough cases confirmed in Nebraska.** Three cases of whooping cough have been confirmed at Mary Lanning Memorial Hospital, in Hastings, NE, in children ranging in age from infancy to 12 years old, a hospital official says. Federal health officials have said cases of whooping cough have been increasing in the U.S. since the 1980s. In 2003 there were 15 reported cases of whooping cough in Nebraska. More than 100 cases were confirmed in Nebraska in 2004. Whooping cough is highly contagious with up to 90 percent of susceptible household contacts developing the infection. It is spread through liquid droplets from an infected person's coughing.
Source: http://abcnews.go.com/US/wireStory?id=628749

24. *March 30, Centers for Disease Control and Prevention* — **What is Marburg hemorrhagic fever?** Marburg is a rare, severe type of hemorrhagic fever affecting both humans and non−human primates. Marburg is caused by a genetically unique zoonotic, or animal−borne, RNA virus of the filovirus family of which the four species of Ebola virus are the only other known members. While the exact native area of the disease is unknown, this area appears to include parts of Uganda, Western Kenya, and perhaps Zimbabwe. As with Ebola virus, the actual animal host for Marburg is unknown, as is the detailed mechanism for transmission from animals to humans. Preventive measures against transmission from the original animal host have not yet been established. Individuals have become infected through handling infected monkeys and direct contact with their fluids or cell cultures. Spread of the virus between humans has occurred in a setting of close contact, often in a hospital, possibly through droplets of body fluids or direct contact with persons, equipment, or other objects contaminated with infectious blood or tissues. After an incubation period of 5−10 days, the onset of the disease is sudden and is marked by fever, chills, headache, and myalgia. Because many of the symptoms of Marburg are similar to those of other infectious diseases, such as malaria or typhoid fever, diagnosis can be difficult. The case−fatality rate is between 23−25%, and a specific treatment is unknown.

Marburg is a rare human disease, but when it does occur, it has the potential to spread to other people, especially health care staff and family members who care for the patient. Therefore, increasing awareness among health−care providers of clinical symptoms in patients that suggest Marburg hemorrhagic fever is critical.
Source: http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/marburg. htm

25. *March 30, Wake Forest University Baptist Medical Center* — **Scientists seek answers on what activates anthrax spores.** Scientists at Wake Forest University Baptist Medical Center and three other institutions are setting out to find what activates the spores in anthrax. "A key aspect of anthrax spore biology concerns the germination process through which the dormant spore

becomes a reproductive, disease−causing bacterium," explained Al Claiborne, the principal investigator. "Basic understanding of the regulatory signals that promote germination will enable discoveries leading to drugs that block the process." The research stems from lessons learned from studying the bacteria that cause Staphylococcus infections and two other bacteria in the same group as anthrax. Claiborne said the group proposes that a vitamin B5 derivative known as Coenzyme A plays a crucial role in the germination of the anthrax spores. They have already shown that anthrax is missing a similar cofactor called glutathione. The genome sequences of four strains of the bacteria, known scientifically as Bacillus anthracis, have been determined. The group also will be exploring the three−dimensional structures and the functions of the proteins involved. Once they know the structures, they may not only be able to provide new details on how anthrax develops, but also pick out structural vulnerabilities that are key to designing new therapeutic agents to prevent anthrax.
Source: http://www1.wfubmc.edu/news/NewsArticle.htm?Articleid=1565

26. *February 28, Government Accountability Office* — **GAO−05−239: Bioterrorism: Information on Jurisdictions' Expenditure and Reported Obligation of Program Funds.** The Department of Health and Human Services' (HHS) Centers for Disease Control and Prevention (CDC) fund jurisdictions' efforts to prepare for bioterrorism attacks through the Public Health Preparedness and Response for Bioterrorism program. Citing jurisdictions' unexpended program funds, HHS reallocated some fiscal year 2004 funds to support other local and national bioterrorism initiatives. The Government Accountability Office (GAO) was asked to provide information on the extent to which jurisdictions had expended funds awarded in various fiscal years and budget periods. As of August 30, 2004, jurisdictions had expended over four−fifths of the fiscal year 2002 funds awarded during the third budget period through the HHS P accounts −− the public assistance accounts that track over 90 percent of all funds awarded. As of that date, they had expended slightly over half of P account funds awarded for the program's fourth budget period. At the end of the program's third budget period, jurisdictions reported that less than one−sixth of all bioterrorism funds awarded for that period −− including both fiscal year 2001 and 2002 funds −− remained unobligated, and some jurisdictions reported that none of their funds remained unobligated. As of August 1, 2004, jurisdictions estimated that less than one−quarter of all funds awarded for the fourth budget period would remain unobligated as of August 30, 2004.
Source: http://www.gao.gov/new.items/d05239.pdf

[Return to top]

Government Sector

27. *March 31, Department of Homeland Security* — **Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction released.** Department of Homeland Security (DHS) Secretary Michael Chertoff issued the following statement on the Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction: “The Department of Homeland Security, in its first two years of existence, has established a comprehensive system to distribute threat information to state and local and law enforcement officials throughout the country so we are better able to protect our communities and the homeland. Although these efforts have made America safer, we welcome the Report of the Commission on the Intelligence Capabilities of

the United States Regarding Weapons of Mass Destruction and look forward to reviewing its recommendations. This month we initiated a complete review of the Department in an effort to ensure we are best organized to manage the threats we face, our vulnerabilities and the consequence of terrorist actions. While we consider the future form and function of DHS, this report will serve as another tool to guide our decision−making to better manage risk, enhance our detection capabilities and improve our intelligence analysis. The Department supplies, consumes, analyzes, and distributes intelligence information, and we are always seeking new ways to apply intelligence to our vulnerabilities to make the homeland more secure." Report: http://www.wmd.gov/report/
Source: http://www.dhs.gov/dhspublic/display?content=4419

[Return to top]

Emergency Services Sector

28. *March 31, Peninsula Daily News (WA)* — **Mock bioterror attack tests officials' skills.** The first countywide public health emergency exercise was held Wednesday, March 31, by the Jefferson County Emergency Operation Center in Washington. The scenario included the release of a biological agent during a motorcycle convention. Participants return home, unknowingly spreading a deadly airborne flu virus to the North Olympic Peninsula's population. About 25 officials and representatives from county and city law enforcement agencies, public health, fire and administrative services spent a full day of sharpening skills for an emergency response. "It went fairly well," said Daphne Kilburn, Jefferson County Emergency Management's public information officer. "We saw some gaps in our communication process−−a couple of minor discrepancies, like assigning specific telephones to an agency and using more written communication messages as opposed to verbal," she said.
Source: http://www.peninsuladailynews.com/sited/story/html/202816

29. *March 31, The Register−Mail (IL)* — **Emergency units handle bio−hazard test.** Emergency response agencies in Galesburg, IL, worked together Wednesday, March 31, during a yearly emergency drill to test readiness. The year's drill was a simulated anthrax attack at Silas Willard Elementary School. Hospital officials were alerted when they noticed several people with flu−like symptoms in their emergency rooms. All of the victims had attended an event at Silas Willard on Sunday, David Adcock, a spokesman for St. Mary Medical Center said at a news conference Wednesday afternoon. He said the school was searched and biological material was found in the sprinkler system.
Source: http://www.register−mail.com/news/local/b60lj810gid.html

[Return to top]

Information Technology and Telecommunications Sector

30. *March 31, Associated Press* — **Federal government completes Internet traffic report.** The National Research Council's report "Signposts in Cyberspace," was released to the public on Thursday, March 31. The council concluded that the Internet's behind−the−scenes address scheme, called its domain name system, is remarkably robust and suitable to meet the Web's

future needs. It urged minor technical improvements to secure the system from hackers and prevent outages from natural disasters, such as moving some of the Internet's 13 key traffic−directing computers outside Washington and Los Angeles. It also recommended those traffic−directing computers continue to be operated by volunteers, organizations and corporations around the world rather than governments. And it advocated dozens of new Internet address suffixes – similar to ".com" and ".net" – be introduced each year to allow for new Websites and e−mail addresses. Report: http://www.nap.edu/catalog/11258.html
Source: http://abcnews.go.com/Technology/wireStory?id=629274

31. *March 30, eWeek* — **Grid computing can allow security threats.** Security experts on Wednesday, March 30, recommended that IT administrators clearly identify and understand the security risks associated with large−scale grid computing deployments. During Ziff Davis Media's Enterprise Solutions Virtual Tradeshow, the pros and cons of grid computing and safe data storage took center stage, with panelists stressing the importance of using best practices to protect the confidentiality of information passed over corporate grid systems. Lenny Mansell, senior security consultant at Triad Information Security Services LLC, warned that greater sharing of information and resources across traditional trust boundaries will result in increased risks that must be addressed as a matter of urgency. Mansell recommends that businesses deploying grid systems identify critical assets and the threats to those assets. Mark Teter, chief technical officer of Advanced Systems Group LLC, said the highly automated manner in which resources are allocated on a grid can be used by a malicious attacker to steal sensitive corporate data. Grid computing is the concept of using computers in the way that utilities use power grids to tap the unused capacity of a vast array of linked systems. Users can then share computing power, databases and services online.
Source: http://www.eweek.com/article2/0,1759,1780849,00.asp

32. *March 30, Government Computer News* — **Massive federal wireless project delayed.** The federal government has advised prospective vendors that it has delayed its schedule and changed its requirements for a multibillion−dollar makeover of federal wireless voice and data communications. In a 25−page amendment to the request for proposals for the Integrated Wireless Network (IWN), Justice Department procurement officials extended the due date for proposals and asked vendors to submit two types of cost proposals based on different deployment plans. These changes follow a proposal amendment issued March 2 that extended the potential duration of the project, which has an estimated cost of $10 billion, from five years to up to 15 years. IWN program Website: http://www.usdoj.gov/jmd/iwn/
Source: http://www.gcn.com/vol1_no1/daily−updates/35400−1.html

33. *March 30, Secunia* — **Sylpheed MIME−encoded attachment filename buffer overflow.** A vulnerability has been reported in Sylpheed, which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error when displaying messages containing attachments with MIME−encoded filenames. This can be exploited to cause a buffer overflow via a specially crafted message. Update to version 1.0.4: http://sylpheed.good−day.net/
Source: http://secunia.com/advisories/14756/

34. *March 30, FrSIRT Advisory* — **E−Store Kit−2 PayPal Edition XSS and PHP file inclusion vulnerability.** Two vulnerabilities were identified in E−Store Kit−2 PayPal Edition, which may

be exploited by attackers to include arbitrary files or conduct Cross Site Scripting attacks. The first flaw resides in the "catalog.php" file, when handling specially crafted "main" and "menu" parameters, which may be exploited by a remote attacker to include arbitrary PHP files and execute commands with the privileges of the web server. The second vulnerability is due to an input validation error in the "downloadform.php" script when handling a specially crafted "txn_id" parameter, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. There is no solution at this time.
Source: http://www.frsirt.com/english/advisories/2005/0298

35. *March 30, FrSIRT Advisory* — **Multiple Telnet clients buffer overflow vulnerabilities.** Two vulnerabilities were identified in several Telnet clients, which may be exploited by attackers to execute arbitrary commands. The first flaw is due to a heap overflow error in the "env_opt_add()" function (telnet.c), which may be exploited to execute arbitrary commands in the context of the user who launched the telnet client. The second vulnerability is due to a buffer overflow error when handling LINEMODE suboptions and processing replies containing a large number of SLC (Set Local Character) commands, which may be exploited to execute arbitrary commands in the context of the user who launched the telnet client. Solutions available through Source link below.
Source: http://www.frsirt.com/english/advisories/2005/0300

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.
Symantec product engineers confirmed both issues impacting Symantec's Auto−Protect feature in Symantec Norton AntiVirus and have developed and released a patch for all impacted products through Symantec LiveUpdate. Customers running Automatic LiveUpdate should already be updated. To manually update via Symantec LiveUpdate, users should run LiveUpdate until all available Symantec product updates are downloaded and installed.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 6346 (gnutella−svc), 135 (epmap), 22321 (wnn6_Tw), 1025 (−−−), 1026 (−−−), 139 (netbios−ssn), 1027 (icq), 80 (www), 53 (domain)

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

36. *March 31, The Buffalo News (NY)* — **Suspected bomb plan thwarted.** Law enforcement officials say they have thwarted a plan to bomb Sweet Home High School in Amherst, NY, with the arrest of a 15−year−old sophomore who had bomb−making materials and told friends he planned to use them at his school. A police search of the boy's Town of Tonawanda home turned up piping bound with duct tape, ball bearings from roller blade wheels and fuse material he purchased at a hardware store. The boy also reportedly bought two pounds of gunpowder from a local drug dealer, and was seeking to purchase more but did not have the money. Prosecutors said the student told friends he planned to bomb the school after Christmas break of his senior year, and that he would give his friends three minutes advance notice. "This obviously had gone far beyond the mere planning stage," said District Attorney Frank J. Clark. "He had obviously gotten the materials together and had stated an intent to use them. We've already had too many cases where these things are carried through to fruition. We don't have the luxury of not taking them seriously.”
Source: http://www.buffalonews.com/editorial/20050331/1053260.asp

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary 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.