Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 13 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 Reed Elsevier Group PLC has said that up to 10 times as many people as originally thought may have had their profiles stolen from a LexisNexis database. (See item 6)
- The Washington Post reports three men, being held on terrorism charges in the United Kingdom, have also been indicted in the United States on charges they planned to blow up financial buildings in Washington, New York, and New Jersey. (See item 8)
- Federal Computer Week reports Federal Emergency Management Agency officials are testing digital technology that can transmit text, voice and video messages simultaneously to wireless devices, radios, televisions, and the Internet. (See item 28)
- Microsoft has released its security bulletins for April 2005. There are five "Critical" and three "Important" updates. A patch is available on the Microsoft Website. (See item 31)

DHS/IAIP Update *Fast Jump*

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 08, Government Accountability Office* — **GAO−05−339: Nuclear Regulatory**

Commission: NRC Needs to Do More to Ensure that Power Plants Are Effectively Controlling Spent Nuclear Fuel (Report). Spent nuclear fuel −− the used fuel periodically removed from reactors in nuclear power plants −− is too inefficient to power a nuclear reaction, but is intensely radioactive and continues to generate heat for thousands of years. Potential health and safety implications make the control of spent nuclear fuel of great importance. The discovery, in 2004, that spent fuel rods were missing at the Vermont Yankee plant in Vermont generated public concern and questions about the Nuclear Regulatory Commission's (NRC) regulation and oversight of this material. The Government Accountability Office (GAO) reviewed (1) plants' performance in controlling and accounting for their spent nuclear fuel, (2) the effectiveness of NRC's regulations and oversight of the plants' performance, and (3) NRC's actions to respond to plants' problems controlling their spent fuel. GAO recommends that NRC (1) establish specific requirements for the control and accounting of loose rods and fragments and plants' conduct of their physical inventories and (2) develop and implement appropriate inspection procedures to verify plants' compliance with the requirements. Commenting on the draft report, NRC generally agreed with GAO's conclusions and recommendations.
Highlights: http://www.gao.gov/highlights/d05339high.pdf
Source: http://www.gao.gov/new.items/d05339.pdf

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *April 12, WFIE (IN)* — **Ammonia leak prompts officials to shut down businesses and schools in Indiana town.** The entire town of Haubstadt, IN, was shut down the morning of Tuesday, April 12, because of an ammonia leak. No one was allowed in or out of the town after a gas was noticed at R and C Farm Supply Company. The company owner said the leak came from a ruptured hose near a loading area. Businesses and schools, including the Haubstaudt Community School, were forced to seal off their buildings from the air. Principal Sheila Meyer said the sheriff's department called and asked school administrators to bring the kids in and completely shutdown the building. The leak was contained within an hour. And no one was hurt.
Source: http://www.14wfie.com/Global/story.asp?S=3194081&nav=3w6oYXp J

[Return to top]

Defense Industrial Base Sector

3. *April 12, IDG News Service* — **Venezuelan arrested for Air Force hacks.** A popular Venezuelan hacker known as RaFa was arrested April 2 and charged with hacking into U.S. Department of Defense servers almost four years ago. RaFa, otherwise known as Rafael Nunez−Aponte, was arrested at Miami International Airport by agents of the Pentagon's Defense Criminal Investigative Service for attacks on computer systems in 2001. Allegedly a member of the hacker group World of Hell, Nunez−Aponte is awaiting transfer to Denver to face one count each of unlawfully accessing a private government computer and causing intentional damage to a protected computer. Nunez−Aponte is believed to be the person behind a June 2001 Web defacement attack on computers belonging to the Pentagon's Defense

Information Systems Agency (DISA). In that attack, Nunez−Aponte allegedly accessed the computers and altered a DISA Webpage, according to a copy of the indictment filed in U.S. District Court for the District of Colorado. He is also alleged to have deleted logging information from the DISA computers and rendered some DISA systems inaccessible to Air Force personnel, according to the indictment.
Source: http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,101026,00.html

[Return to top]

Banking and Finance Sector

4. *April 12, Star−Telegram (TX)* — **Police in Texas county warn voters of identity theft.** More than 600 Tarrant County, TX, voters have been notified that they may have been the victim of identity theft after Garland police found that a suspect possessed internal voter registration information. There are 860,000 registered voters in Tarrant County. The letters sent by Garland police were issued just a few weeks after Precious China, 25, of Garland, was arrested on a fraud warrant, Garland police spokesperson Joe Harn said. "Voter printouts were found on her," Harn said. "And we became concerned when we found three names highlighted." Investigators have not determined how China got the list, Harn said. Gayle Hamilton, Tarrant County's assistant elections administrator, said China was not an employee of Tarrant County. Hamilton said the May 2004 printout contained information about new voters and people who had updated their registrations. The lists are generated each week, and until recently the old lists were thrown away, she said. Hamilton said election officials now shred the document before discarding it. "We don't know how she got it," Hamilton said. The printout included the Social Security and driver's license numbers of some voters, items that are optional when filling out voter applications, Hamilton said. "That list was just for office use," Hamilton said.
Source: http://www.dfw.com/mld/dfw/news/local/11373527.htm

5. *April 12, Finextra Research* — **U.S. banks to upgrade identity theft center.** The U.S. bank−backed Identity Theft Assistance Center (ITAC) is to be permanently established as a free service to consumers after helping restore financial identities to nearly 700 victims of identity theft during a one−year pilot. Funded by banking members of the Financial Services Roundtable and Bits, ITAC was set up to streamline the recovery process for victims of identity theft and to share information with law enforcement bodies. Steve Bartlett, resident and CEO of the Roundtable, says the ITAC service is currently being enhanced “so it can be as responsive as possible to victims' needs and move us toward our other objective − using the information to prosecute and convict identity thieves.” The ITAC walks the consumer through his or her credit report to find suspicious activity, notifies the affected creditors and places fraud alerts with the credit bureaus.
Identity Theft Assistance Center: http://www.identitytheftassistance.org/home/index.cfm
Source: http://www.finextra.com/fullstory.asp?id=13501

6. *April 12, Associated Press* — **LexisNexis breach may be worse than thought.** Up to 10 times as many people as originally thought may have had their profiles stolen from a LexisNexis database in the U.S., publisher and data broker Reed Elsevier Group PLC said Tuesday, April 12. The company reported last month that criminals may have accessed personal details of

32,000 people via a breach of LexisNexis' recently acquired Seisint unit. It now says that figure is closer to 310,000 people. Reed said it had identified 59 incidents since January 2003 in which unauthorized persons, predominantly using IDs and passwords of legitimate Seisint customers, may have fraudulently acquired personal identifying information on those thousands of people. Reed spokesperson Patrick Kerr said the company uncovered the first batch of breaches during a review and integration of Seisint's systems shortly after it purchased the unit in August. Seisint stores millions of personal records, including individuals' addresses and Social Security numbers. The company said the 59 identified incidents −− 57 at Seisint and two in other LexisNexis units −− largely related to the misappropriation by third parties of IDs and passwords of legitimate customers and stressed that neither LexisNexis nor the Seisint technology infrastructure was breached by hackers. The Senate Judiciary Committee will address legislation on this issue during a hearing Wednesday morning.
Official Reed Elsevier Group PLC Press Release:
http://www.reed−elsevier.com/index.cfm?articleid=1319
Senate Judiciary hearing "Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use:"
http://judiciary.senate.gov/hearing.cfm?id=1437
Source: http://www.nytimes.com/aponline/business/AP−LexisNexis−Data− Breach.html?

7. *April 12, CNET news.com* — **Phishing twist relies on bogus blogs.** A new form of phishing is taking shape and riding on the growing popularity of blogs, security company Websense said Tuesday, April 12. Malicious virus writers are attempting to lure people to malicious blogs using enticing e−mails and instant messages, according to a statement from Websense. Once a person arrives at the blog, which can be posted on a legitimate host site, the victim's computer becomes infected with software designed to steal sensitive information, such as passwords and bank account information. "These aren't the kind of blog Websites that someone would stumble upon and infect their machine accidentally," said Dan Hubbard, Websense senior director of security and technology research. In one recent case, Websense found a spoofed e−mail that tried to lure people to a malicious blog that would run a Trojan horse. The e−mail looked like it came from a popular instant−messaging service, and it tried to entice the recipient to click on a link to get a new version of its IM program. But when people clicked on the link, it directed them to a blog that hosted keystroke−logging software to steal their passwords when they accessed certain online banking sites.
Source: http://news.com.com/Phishing+twist+relies+on+bogus+blogs/2100−7349_3−5666617.html?tag=nefd.top

8. *April 12, Washington Post* — **Three indicted for plot to attack financial institutions.** Three men who are being held on terrorism charges in the United Kingdom have also been indicted in the United States on charges that they planned to blow up financial buildings in Washington, DC, New York, and New Jersey, according to court documents unsealed Tuesday, April 12. The four−count indictment filed in U.S. District Court in Manhattan alleges that Dhiran Barot, Nadeem Tarmohammed and Qaisar Shaffi took part in months of methodical reconnaissance of financial targets between August 2000 and April 2001. The eight−page indictment provides the fullest official picture yet of the alleged plot, which led to a terrorism alert last August after authorities discovered evidence of surveillance on a computer seized in Pakistan. The three defendants are already in custody in Great Britain on related charges that they possessed reconnaissance plans and other information useful in conducting a terrorist attack. Authorities

have said the group was also working on a plan targeting London's Heathrow Airport.
Source: http://www.washingtonpost.com/wp−dyn/articles/A46550−2005Apr 12.html

9. *April 11, ZDNet Australia* — **Site−blocking worm carries phishing risk.** A new variant of the Crowt worm could block infected browsers from accessing Websites belonging to some antivirus sellers, Trend Micro has warned. Crowt.D, first discovered Wednesday, April 6, opens up the Google News site upon infection, then alters the computer's hosts file to add a list of Website addresses, the antivirus company said in an advisory. When people click on one of those addresses, they are redirected to a local loopback address instead, a move that blocks access to the sites in the list. The worm restricts access to antivirus vendor sites including Trendmicro.com, Kapersky−labs.com, Sophos.com, Symantec.com and Us.mcafee.com. Adam Biviano, senior systems engineer at the company, said the worm is noteworthy because it has the potential to send a victim to a phishing Website even when they have manually typed in a Web address. The Crowt.D infection's ability to redirect people from one Website to another is especially dangerous when it involves an online banking service, Biviano said. "Banks are telling their customers to type their specific Website address into the browser. However, if the host file has been compromised, then even if the URL is typed in, the browser will still go to the phishing Website," Biviano said.
Source: http://news.zdnet.com/2100−1009_22−5662922.html

10. *April 11, KVBC (NV)* — **Secret Service investigates counterfeit bills in Nevada.** A counterfeit ring is operating in Nevada that involves 10−dollar bills. Over fifty thousand in fake bills were used in slot machines at several casinos and convenience stores in Las Vegas, Laughlin, and Reno. The bill validators inside some machines aren't recognizing the fake bills. Because the machines are accepting the fake bills, Secret Service agents are relying on casino security and store clerks to be on the lookout for suspicious activity. At least two casinos in Laughlin aren't accepting 10−dollar bills while this scam is being perpetrated.
Source: http://www.kvbc.com/Global/story.asp?S=3196443&nav=15MVYXlc

11. *April 08, JoongAng Daily (Korea)* — **New computer viruses seeking financial data.** Recent computer viruses and worms in Korea are hacking into personal computers to access financial information, such as credit card numbers, bank account numbers and related passwords. Although personal computers have always been subject to various infections, current viruses are different in that they are not just pranks, but have specific hacking functions. A few years ago, most viruses disabled basic functions of computers, bogging down the computer's processing speed or mess up the system and delete or duplicate files at random. Recent variants, however, are programmed to silently search for personal financial information and are therefore harder to detect. Security experts said that these bugs are increasing because more Koreans are performing financial duties online without protection. "Home banking, cyber stock trading and online shopping have increased greatly in the past few years; therefore, more personal financial data are installed in computers," said Yoon Gwang−taik, an official at computer security firm Symantec Corp.
Source: http://www.snpx.com/cgi−bin/news55.cgi?target=90954039?−1313

12. *April 06, Jerusalem Post (Israel)* — **Hacker who cracked bank's computer code sentenced.** David Sternberg, a hacker who managed to break into the computer network of the Postal Bank in Israel and transfer large sums of money to the accounts of co−conspirators, was sentenced to

16 months in prison by the Haifa magistrate's court on Wednesday, April 6. It started with a mysterious break−in at the Postal Bank branch office in the Dania housing district of Haifa. Bank officials reported the apparent burglary but found that nothing had been stolen and the case was closed. In fact, Sternberg had opened the communications box in the bank and connected a remote controlled "access point" device to the computer network. "This gave him instant access to all of the bank's accounts and transactions nationwide," said Supt. Herby Frimet of the Northern Region White Collar Fraud Squad. Frimet said that in the interim Sternberg had made arrangements with six accomplices who either had accounts with the bank or opened new ones to which Sternberg transferred money from other accounts. The computer fraud came to light when officials at the Tel Aviv head office of the bank noticed that certain amounts of money were being transferred on a regular basis from the bank's main account to those of certain individuals.
Source: http://www.jpost.com/servlet/Satellite?pagename=JPost/JPArticle/ShowFull&cid=1112754019642

[Return to top]

Transportation Sector

13. *April 12, Associated Press* — **Lasers to warn pilots away from restricted airspace near the U.S. Capitol.** Pentagon officials said Monday, April 11, that lasers will be used to warn pilots when they've flown into restricted airspace near the Capitol, even though federal officials have warned that terrorists might use the beams of light to blind pilots as they approach airports. There have been more than 100 incidents nationwide since November in which laser beams have been flashed into cockpits. The aircraft all landed safely, but federal aviation officials are concerned that a laser could be used to blind pilots and cause a crash. The North American Aerospace Defense Command, or NORAD, said its laser warning system will start in 30 to 45 days. The low−intensity lights are less powerful than the ones that prompted warnings, and tests have shown they are safe for the eyes, according to NORAD spokesperson Michael Kucharek who said the laser−based warning system someday could replace fighter jets as a way to warn pilots to stay away from the Capitol and the White House. In some cases, NORAD has had to divert or scramble fighter jets to escort small private planes that have strayed into the restricted airspace in Washington, DC, at a cost of $30,000 to $50,000 each time.
Source: http://www.cnn.com/2005/TRAVEL/04/12/lasers.planes.ap/index. html

14. *April 12, Washington Post* — **Road projects may be rekindled to meet security needs.** From nearly the moment that Virginia's Arlington County portion of Interstate 66 opened in 1982, various planners and officials have fought to widen it based on the simple argument that more lanes are needed to alleviate daily traffic jams. The latest effort to widen the road, launched last year on Capitol Hill and under consideration by Virginia officials, includes another justification: that a third westbound lane would help people flee Washington in the event of another terrorist attack. The I−66 widening is one of billions of dollars' worth of stalled or contentious road and transit projects −− some that were conceived of decades ago and others far from dense population centers −− that state officials and highway advocates across the region are reselling in part as evacuation routes. Nevertheless, officials across the region have concluded that the most likely type of threat would be limited in area. So they have adopted a strategy of dealing with the affected area first and instructing others to "shelter in place" until

they are given the all−clear to head home.
Source: http://www.washingtonpost.com/wp−dyn/articles/A40440−2005Apr 9.html

15. *April 12, Department of Homeland Security* — **Grants to secure transit.** The Department of Homeland Security (DHS) on Tuesday, April 12, announced $141,630,806 in transit security grants. The Transit Security Grant Program (TSGP) provides for the protection of regional transit systems and the commuting public from terrorism, especially explosives and non−conventional threats. The program totals $135,257,076 for owners and operators of some of the nation's most critical infrastructure, including: $107,900,000 for rail transit systems, $22,357,076 for intra−city bus systems, and $ 5,000,000 for ferry systems. DHS designed this program in coordination with federal partner agencies and industry, including the U.S. Department of Transportation, owners and operators of the nation's mass transit systems, and the American Public Transportation Association. The Department is also awarding $6,373,730 to Amtrak through the Intercity Passenger Rail Security Program (IPRSGP) for security enhancements for intercity passenger rail operations in the Northeast Corridor and at Amtrak's hub in Chicago, IL. The grant programs specifically provide funding for the prevention and detection of explosive devices and chemical, biological, radiological and nuclear agents.
FY 2005 Transit Security Grant Program Allocations (PDF, 4 pages − 245 KB):
http://www.dhs.gov/dhspublic/interweb/assetlibrary/Grants_FY 2005TSGPAllocations_4−12−05.pdf
Source: http://www.dhs.gov/dhspublic/display?content=4447

16. *April 12, TheDenverChannel.com* — **United CEO wants airline to eliminate pension plans.** United Airlines CEO Glenn Tilton reiterated the carrier's intent Monday, April 11, to eliminate unionized employees' current pension plans and replace existing labor contracts as necessary to obtain bankruptcy exit financing. Escalating fuel prices have left the airline in no position to compromise on its cutback plans, Tilton said. United, a unit of Elk Grove Village, IL−based UAL Corp., said in a bankruptcy filing Monday that it intends to replace existing pensions and tear up collective bargaining agreements with the mechanics and machinists unions if they don't agree to permanent pay cuts and other concessions by a May 11 trial date. In its filing, the company argued that it has found no alternatives to ending the pension plans and replacing labor contracts. The airline said it "shares its employees' frustration" over having to take the step. Tilton said United is still targeting this fall for emerging from Chapter 11 bankruptcy, but only if it is able to reduce costs enough to satisfy banks that have expressed interest in providing $2 billion to $2.5 billion in exit financing. He characterized contract negotiations as "rigorous."
Source: http://www.thedenverchannel.com/money/4371736/detail.html

17. *April 12, Associated Press* — **Engine part falls from Northwest flight bound for Hawaii.** An engine part on a Northwest Airlines jet bound for Hawaii fell off the aircraft and landed in a Dakota County, MN, field, the Federal Aviation Administration (FAA) confirmed Monday, April 11. Elizabeth Isham Cory, a spokesperson for the FAA, said Flight 97 left Saturday, April 9, from Minneapolis−St. Paul International airport bound for Honolulu. The flight crew didn't notice that the cone−shaped engine part −− called a thrust reverser nozzle −− was missing until the DC−10 had landed, she said. No one was injured. The thrust reverser helps to slow planes when they come in for a landing. The landing in Hawaii was routine, Isham Cory said. She referred to the engine part that fell, which is located on the tail of the aircraft, as an "extra

mechanism" that wasn't being used in the flight. The Dakota County sheriff notified the FAA after a resident who saw the piece fall to the ground called Inver Grove Heights police, she said. The FAA later retrieved the engine part, which weighed about 200 pounds. "This is very rare," Isham Cory said. "We are trying to decide how it happened, why it happened and what steps can be taken to prevent it from happening on another plane."
Source: http://www.usatoday.com/travel/flights/2005−04−12−nwa−engine_x.htm

18. *April 12, Transportation Security Administration* — **Explosives detection trace portal deployed to Phoenix Sky Harbor International Airport.** The Transportation Security Administration (TSA) announced that Phoenix Sky International Airport (PHX) will receive a new explosives detection trace portal to screen passengers at the new Terminal 4A security checkpoint, starting Tuesday, April 12. The equipment is part of a pilot program to test and evaluate the trace portal for screening passengers for explosives. At Phoenix, some passengers will be directed by the TSA screeners to step into the trace portal. Passengers will stand still for a few seconds while several “puffs” of air are released. The portal will collect and analyze the air for traces of explosives and a computerized voice will tell passengers when to exit. Even as the pilot program continues, TSA has allocated $28.3 million to purchase and install an additional 147 trace portals. TSA is currently developing a purchase and deployment plan to have the equipment in airports by January 2006. Once the plans are finalized, TSA will announce the next group of airports to receive the equipment.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 0117295

[Return to top]

Postal and Shipping Sector

19. *April 12, WJRT−TV (MI)* — **Michigan post office receives new screening gear.** Sophisticated detection equipment will be installed in Flint, Michigan's main post office Saturday, April 16. Flint is getting a "Biohazard Detection System" that will identify anthrax. The machine gently squeezes each letter to search for anthrax. The new machine doesn't work on packages. The Postal Service is confident it's a good system and claims that so far, they've never had a false alarm.
Source: http://abclocal.go.com/wjrt/news%5C041105_NW_da_postal.html

[Return to top]

Agriculture Sector

Nothing to report.
[Return to top]

Food Sector

20. *April 11, Food Safety and Inspection Service* — **Turkey and pork products recalled.** L.S.K. Smoked Turkey Products, Inc., a Bronx, NY, firm, is voluntarily recalling approximately 39,000 pounds of smoked turkey and pork products that may be contaminated with Listeria

monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Monday, April 11. The products were shipped to distribution centers in Delaware, New Jersey, New York, and Florida for institutional use. The problem was discovered through FSIS regulatory sampling. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_017_2005_Relea se/index.asp

21. *April 11, Food Safety and Inspection Service* — **Sausage products recalled.** Roger Wood Foods, Inc., a Savannah, GA, firm, is voluntarily recalling approximately 10,700 pounds of sausage products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Monday, April 11. The sausage was distributed to retail stores in Florida, Georgia, North Carolina, and South Carolina. The problem was discovered through regulatory sampling conducted by the State of Georgia. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_018_2005_Relea se/index.asp

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

22. *April 12, New York Times* — **Tracking the Marburg virus in Angola.** The staff in the pediatric ward of Uíge's regional hospital suspected something was wrong as early as October, when children who had been admitted with seemingly treatable illnesses began to die. International health experts say they cannot pinpoint exactly when the outbreak of the Marburg virus began. But local officials in Uíge, the center of the outbreak, believe it began around October, and then spread from the pediatric ward of the regional hospital. If they are correct and there was a delay in explaining the deaths, the reason may be that in Africa, sometimes the extraordinary is buried in the ordinary. Children die at such an astonishing pace there and for any range of horrible reasons unknown to other parts of the world that it takes much more time for health workers to piece together if something as deadly as Marburg is at work. In a country like Angola, where one in four children dies before the age of five, mostly from infectious diseases, crises like the one in the pediatric ward can easily be overlooked. By the end of December, at least 95 children were dead. It was not until early March that the provincial health officials alerted a World Health Organization (WHO) representative that they had found suspected cases of Marburg.
Source: http://www.nytimes.com/2005/04/12/health/12angola.html?oref= login

23.

April 12, Canadian Press — **C. difficile strain shows 20−fold toxin increase over other strains.** The strain behind the C. difficile outbreak plaguing some Quebec, Canada, hospitals generates 20 times the toxins produced by many other strains of the bacteria, U.S. and Canadian scientists are reporting. Using samples isolated from patients in Sherbrooke, Quebec, research scientists at Acambis Inc., a biotechnology firm in Cambridge, MA, were able to discover the enormous toxin−generating powers of the strain, believed to have caused or contributed to the deaths of more than 200 people in Quebec in recent years. Researchers caution they haven't proven that the increased toxin production is behind the hypervirulence of the strain. But they believe it is playing a role in the high degree of severe disease associated with this particular strain of C. difficile. The study is being presented at the annual meeting of the Society for Healthcare Epidemiology of America in Los Angeles, CA.
C. difficile information: http://www.cdc.gov/ncidod/hip/gastro/ClostridiumDifficile.ht m
Source: http://www.canada.com/health/story.html?id=4fa72bf3−0028−4fb a−8ed5−034b58e9b003

24. *April 12, Knight Ridder Newspapers* — **Senate looks at expanding patents for bioweapon antidotes.** The U.S. Senate is looking to enact incentives for drug companies to develop medicines to protect against biological attacks and epidemics. Sens. Judd Gregg, Bill Frist, and Rick Santorum are sponsoring one bill. Sens. Joe Lieberman and Orrin G. Hatch plan to introduce their own version, with even broader patent extensions. President Bush signed BioShield legislation that called for tax breaks and $5.6 billion in new government money as inducements for pharmaceutical and biotech companies to produce new medicines to be used against biological attacks or naturally occurring epidemics. But Gregg and others say the response of big pharmaceutical companies, which have the money and research capabilities to quickly generate new medicines, has been tepid. The problem in responding to such threats, from the perspective of big drug makers, is that the BioShield legislation lacked protections against lawsuits. Drug companies, moreover, complain that the additional funding and tax breaks in the BioShield law are not enough of an incentive. The main reason is that a biological agent that would be used in an attack, or a germ capable of unleashing an epidemic, is by definition a rarity. Thus, a defense against them is less likely to be commercially viable.
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/politi cs/11373735.htm

25. *April 11, United Press International* — **Danish cowpox case might be a warning.** A Danish researcher says a six−year−old case of cowpox infection, which was not publicized at the time, was a warning about viruses in nature and how dangerous viruses might strike without warning. Laurids Siig Christiansen, senior researcher at Denmark's Institute for Food and Veterinary Research, said a 13−year−old Danish boy contracting the disease should be a warning sign to doctors, researchers and the public in general. "The boy is an example of what can happen, when nobody is vaccinated anymore against a certain disease, in this case smallpox, and enormous groups of people are no longer immune to the virus," Christiansen said. "We know of cowpox in Denmark, but there could be other viruses that we don't know about and which, unlike cowpox, are dangerous. We ought to prioritize it higher."
Source: http://washingtontimes.com/upi−breaking/20050411−081148−7904 r.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *April 12, Government Accountability Office* — **GAO−05−530T: Homeland Security: Management of First Responder Grant Programs and Efforts to Improve Accountability Continue to Evolve (Testimony).** In fiscal years 2002 through 2005, the Office for Domestic Preparedness (ODP) within the Department of Homeland Security managed first responder grants totaling approximately $10.5 billion. The bulk of this funding has been for statewide grants through the State Homeland Security Grant Program and urban area grants through the Urban Areas Security Initiative. This testimony provides information on the history and evolution of these two grant programs, particularly with respect to ODP grant award procedures; timelines for awarding and transferring grant funds; and accountability for effective use of grant funds. In prior reports on issues related to federal funding and oversight of grants for first responders, GAO has made recommendations for strengthening federal leadership, cooperation, and planning efforts. These include developing a coordinated strategic plan for use of first responder funds in the National Capital Region and monitor the plan's implementation and using grant guidance to encourage the development of statewide plans for interoperable communications. The National Capital Region and DHS agreed with these recommendations and are working to implement them.
Highlights: http://www.gao.gov/highlights/d05530thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−530T

27. *April 12, The Register−Pajaronian (CA)* — **California county conducts disaster drill.** A drill in Monterey County, CA, on Saturday, April 9, involved emergency officials in 16 fire engines, 11 law agencies, four emergency medical technician agencies and 10 related agencies including the FBI, for a total of 187 responders. The 24−hour drill also included transporting "patients" to two area hospitals. "This is the largest ever drill for this county, and it has taken an enormous amount of preparation," Carmel Fire Chief Sydney Reade said. "The scenario involves three car bombs, possible radiological material, about 40 serious injuries, structural collapse and much more, as the search and rescue unfolds." The cost of the event, funded by a homeland security grant, totaled $121,000, Reade said. Fire Capt. John Hasslinger, who headed up a newly created Urban Search and Rescue crew from North Monterey County Fire, said the drill serves as a valuable tool to help link up multiple agencies in a large−scale disaster.
Source: http://www.zwire.com/news/newsstory.cfm?newsid=14326014&title=%3Cp%3EMonterey%20County%20readies%20for%20disaster&BRD=1197&PAG=461&CATNAME=Top%20Stories&CATEGORYID=410

28. *April 11, Federal Computer Week* — **FEMA officials testing digital alert system.** In an attempt to expand the nation's alert and warning system, Federal Emergency Management Agency (FEMA) officials are testing digital technology that can transmit text, voice and video messages simultaneously to wireless devices, radios, televisions and the Internet. FEMA, which is part of the Department of Homeland Security, is partnering with several agencies on the initiative, called the Digital Emergency Alert System pilot, part of the Integrated Public Alert and Warning initiative. The pilot, which is being conducted in the Washington, DC,

metropolitan area, is testing IP datacasting technology. The one−year test project could determine how the president transmits future messages nationwide during a widespread emergency. But state and local emergency officials could use the digital technology on a daily basis to target encrypted, nearly instantaneous messages at authorized individuals in certain regions during emergencies.
FEMA Website: http://www.fema.gov/
Source: http://www.fcw.com/article88522−04−11−05−Print

29. *April 11, The Caledonian−Record (VT)* — **First responders tested in tabletop drill .** About 75 first responders faced various emergency scenarios in a tabletop exercise Saturday, April 9, in Newport City, VT. Saturday's drill on paper is preparation for a real−time enactment, called Operation Glow, on May 14. The first responders spent a lot of time Saturday morning asking questions about the Operation Glow scenarios crafted by Lt. Tom Hanlon of the Vermont State Police in Derby. They also learned about how their peers, especially in the U.S. Customs and Border Patrol and the railway industry, are prepared to react in emergencies.
Source: http://www.caledonianrecord.com/pages/local_news/story/3b7e9 c00d

30. *April 10, Washington Post* — **Most District terrorism funding not spent.** Although Washington, DC, area is designated as high−risk, it has not spent $120 million of the $145 million in anti−terrorism grants awarded by the federal government over the past three years, including funds earmarked for such critical items as hospital beds and protective gear for rescue workers. Local authorities said that spending fell behind in 2003 and that more time was needed to coordinate plans with Maryland, Virginia and 16 suburban jurisdictions. Local authorities said the ranking is misleading because it does not reflect that they have committed 80 percent of their funds, or $115 million, to projects underway for the District and its suburbs in Maryland and Northern Virginia. The inclusion of obligated funds, they said, is a fairer measure than counting dollars spent only after the work is completed. The region has made some progress. Local governments spent $25 million for baseline needs of police, fire and medical workers, including: obtaining 1,000 radios; starting a public emergency alert system; developing a disease surveillance network; and teaching preparedness to schoolchildren through a Masters of Disaster program. Matt Mayer, acting executive director of the Department of Homeland Security's preparedness office, said Washington faced a unique burden in having to bridge the federal, state and local governments.
Source: http://www.washingtonpost.com/wp−dyn/articles/A40729−2005Apr 9.html

[Return to top]

Information Technology and Telecommunications Sector

31. *April 12, Microsoft* — **Microsoft releases April 2005 security bulletins.** Microsoft released its security bulletins for April 2005. There are five “Critical” (MS05−019 – MS05−023) and three “Important” (MS05−016 – MS05−018) updates. Software affected includes: Windows Server 2003, Windows XP SP1 and SP2, Windows XP 64−Bit Edition SP1 and 2003 (Itanium), Windows 2000 SP3 and SP4, Windows ME, Windows 98 SE, Windows 98, Internet Explorer, Word, Works Suite, Exchange Server 2003, 2003 SP1 and 2000 SP3, and MSN Messenger 6.2. Impact ranges from Denial of Service to remote code execution. Updates are available through the Source link and the US−CERT has provided additional information in "Technical Cyber

Security Alert TA05−102A: Multiple Vulnerabilities in Microsoft Windows Components."
US−CERT Website: http://www.us−cert.gov/cas/techalerts/TA05−102A.html
Source: http://www.microsoft.com/technet/security/bulletin/ms05−apr. mspx

32. *April 11, Secunia* — **Maxthon security ID disclosure vulnerability.** A vulnerability has been reported in Maxthon, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a design error where the security ID of a plug−in is not properly protected from being included and accessed on an external website via the script tag. This can be exploited to read and write arbitrary files via the "readFile()" and "writeFile()" API functions via directory traversal attacks.
Update to version 1.2.2: http://www.maxthon.com/download.htm
Source: http://www.secunia.com/advisories/14918/

33. *April 11, Secunia* — **ModernBill cross−site scripting and file inclusion vulnerabilities.** Some vulnerabilities have been reported in ModernBill, which can be exploited by malicious people to conduct cross−site scripting attacks and compromise a vulnerable system. Input passed to the "c_code" and "aid" parameters in "orderwiz.php" isn't properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Input passed to the "DIR" parameter in "news.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Update to version 4.3.1.
Source: http://secunia.com/advisories/14890/

34. *April 11, FrSIRT Advisory* — **CA BrightStor ARCserve Backup remote buffer overflow vulnerability.** A buffer overflow vulnerability was identified in Computer Associates BrightStor ARCserve Backup UniversalAgent, which may be exploited by remote attackers to execute arbitrary commands. The flaw occurs when handling malformed requests containing a specially crafted "option" field (port 6050/TCP/UDP), which may be exploited by unauthenticated attackers to run arbitrary code with SYSTEM privileges. Refer to Source link for solutions.
Source: http://www.frsirt.com/english/advisories/2005/0334

35. *April 11, National Science Foundation* — **National Science Foundation announces intent to establish cybersecurity center.** The National Science Foundation (NSF) has announced it intends to establish two new Science and Technology Centers (STCs) in fiscal 2005. One is a major collaborative cybersecurity project led by the University of California, Berkeley, and a second, centered at the University of Kansas, will study polar ice sheets. The cybersecurity center will investigate key issues of computer trustworthiness in an era of increasing attacks at all levels on computer systems and information−based technologies. The Team for Research in Ubiquitous Secure Technology (TRUST) will address a parallel and accelerating trend of the past decade–the integration of computing and communication across critical infrastructures in areas such as finance, energy distribution, telecommunications and transportation. The center will lead development of new technologies based on findings from studies of software and network security, trusted platforms and applied cryptographic protocols. Formal approval of the new centers, with funding estimated at nearly $19 million over five years for each center, is still subject to final negotiations between NSF and the lead institutions.
UC Berkeley Press Release: http://www.berkeley.edu/news/media/releases/2005/04/11_trust

.shtml
Source: http://www.nsf.gov/news/news_summ.jsp?cntn_id=103178&org=OLP A&from=news

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 is aware of multiple vulnerabilities that exist within the Groove Virtual Office application suite. Federal Civilian Agencies that utilize this application are encouraged to take actions to minimize the exposure of these systems within their network.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 2234 (directplay), 139 (netbios−ssn), 1026 (−−−), 53 (domain), 80 (www), 1027 (icq), 6881 (bittorrent), 6346 (gnutella−svc) 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. *April 12, ConsumerAffairs.com* — **Senate asked to expand National Mall.** The National Mall should be expanded, made more visitor−friendly and placed under the control of a conservancy or board of regents that would guide and coordinate its future development, architect W. Kent Cooper told a Senate subcommittee on Tuesday, April 12. The National Mall needs a "third−century vision" that would include expansion along South Capitol Street and the L'Enfant Promenade, creating a continuous route from the Capitol to the Lincoln Memorial along a two−mile stretch of the Potomac River, said Cooper, coordinator of the National Mall Third Century Initiative. Cooper noted that today's National Mall is the result of two visions −− the L'Enfant Plan of 1791, which established the portion of the Mall that includes the Washington Monument, and the McMillan Plan of 1901, which resulted in the addition of the section encompassing the Lincoln Memorial. Cooper proposed creation of a National Mall Conservancy that would establish policies for the entire Mall in collaboration with the federal stakeholder agencies and the public, similar to the Smithsonian Institution's Board of Regents.
Source: http://www.consumeraffairs.com/news04/2005/natl_mall.html

[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