Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 08 April 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- IDG News Service reports former employees of a call center in Pune, India, have been arrested on charges of defrauding four account holders in the New York branch of Citibank, a subsidiary of Citigroup, for $300,000. (See item 8)
- The Boston Globe reports Marines preparing for combat in Iraq or Afghanistan have lost significant amounts of training time because undocumented immigrants from Mexico have constantly wandered onto a bombing test range in Yuma, AZ. (See item 11)
- Reuters reports government health agencies are strengthening ties to airlines and aviation regulators to guard against the spread of infectious diseases or other deadly agents aboard commercial aircraft. (See item 22)

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 07, Associated Press* — **Lawmakers: Daylight saving time saves fuel.** Lawmakers crafting energy legislation approved an amendment Wednesday to extend daylight−saving time by two months, having it start on the last Sunday in March and end on the last Sunday in November. "Extending daylight−saving time makes sense, especially with skyrocketing energy costs," said Rep. Fred Upton, R−MI, who along with Rep. Ed Markey, D−MA, co−sponsored

the measure. The amendment was approved by the House Energy and Commerce Committee that is putting together major parts of energy legislation likely to come up for a vote in the full House in the coming weeks. "The more daylight we have, the less electricity we use," said Markey, who cited Transportation Department estimates that showed the two−month extension would save the equivalent of 10,000 barrels of oil a day.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=512&ncid=718 &e=4&u=/ap/20050407/ap_on_go_co/daylight_time

2. *April 07, Triangle Business Journal (NC)* — **Progress completes Brunswick Nuclear Plant work.** Employees of Progress Energy's Brunswick Nuclear Plant, near Southport, NC, completed a scheduled refueling and maintenance outage of one of its two power−generating units on Wednesday, April 6. Brunswick Unit 2 was taken out of service March 4 to replace 44 percent of the reactor's fuel assemblies and to perform numerous maintenance and inspection activities that must be carried out when the reactor is shut down. The Brunswick Plant's two nuclear powered reactors operate on 24−month fuel cycles, with one unit taken out of service for refueling and maintenance each spring.
Source: http://triangle.bizjournals.com/triangle/stories/2005/04/04/ daily25.html

3. *April 07, Free Internet Press* — **China plans to build 40 nuclear power plants.** China plans to build 40 nuclear power plants over the next 15 years, making them the main power source for its booming east coast, a government technology official says. "Nuclear power will play an increasingly important role in the development of China's power industry," said Zhang Fubao, an official of the Commission of Science, Technology and Industry for National Defense, quoted Thursday, April 7, by the official Xinhua news agency. China is expected to be the world's biggest developer of nuclear power stations in coming decades as the government tries to meet soaring demands for electricity while reducing pollution from coal−fired power plants.
Source: http://freeinternetpress.com/modules.php?name=News&file=arti cle&sid=3317

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *April 07, WRIC (VA)* — **Diesel tanker catches fire, fuel spills into river.** A diesel tanker caught fire as it fueled a tugboat on the Elizabeth River in Norfolk, VA, Wednesday, April 6. No injuries were reported but an undetermined amount of fuel spilled. Firefighters arriving on the scene of the two−alarm fire found flames dangerously close to the Bay Towing Corporation's riverfront office building. Crews laid booms to contain the fuel that spilled into the river. Captain Garry Windley, spokesperson for Norfolk Fire−Rescue, said diesel floats on water and crews were able to isolate the spill. Fire crews came from various departments in Hampton Roads, and the Coast Guard responded by boat and helicopter.
Source: http://www.wric.com/Global/story.asp?S=3179009

5. *April 07, Salt Lake Tribune (UT)* — **Chemical cloud keeps some Utah residents inside.** A vapor cloud lingering above Hexcel Corporation's West Valley City, UT, plant prompted the beginning of a large−scale evacuation Wednesday, April 6, but when firefighters realized it was a nontoxic irritant, they instead advised residents to stay inside. Schools and residents

downwind of the carbon fiber manufacturer were alerted just after 7:00 a.m., when overheated epoxy resin created a yellow−brownish plume. Firefighters from seven agencies −− who feared the vapor cloud might be cyanide −− began calling for evacuations, said Fire Captain Bob Fitzgerald. Firefighters eventually discovered the chemical was not poisonous but was more like pepper spray that irritates the eyes, nose and throat. They then advised nearby schools and residents to "shelter in place," or stay inside, until the vapor cloud cleared.
Source: http://www.sltrib.com/utah/ci_2643913

6. *April 07, Patriot News (PA)* — **Truck's leaking cargo prompts closure of truck stop.** The Pilot Truck Stop in Middlesex Township, PA, was closed Wednesday, April 7, for nearly four hours after a flammable liquid was discovered leaking from the trailer of a tractor−trailer rig that had pulled into the truck stop, said John Bruetsch, county public information officer. The trucking company's hazardous response team discovered a drum inside the trailer was leaking, Bruetsch said. The team placed the leaking drum inside another drum, then hauled it and the trailer to another site, he said. No injuries were reported.
Source: http://www.pennlive.com/news/patriotnews/west/index.ssf?/base/news/1112865622244190.xml

[Return to top]

Defense Industrial Base Sector

7. *April 07, Government Accountability Office* — **GAO−05−234: Defense Trade: Arms Export Control System in the Post− 9/11 Environment (Report).** The U.S. government controls arms exports by U.S. companies to ensure that such exports are consistent with national security and foreign policy interests. There have been various efforts to change the arms export control system, which is overseen by the State Department. One effort was the Defense Trade Security Initiative of 2000, which was intended to facilitate defense trade with allies in the post−Cold War environment. Given the September 2001 terror attacks, the U.S. government has had to reevaluate whether existing policies support national security and foreign policy goals. In light of the September 2001 attacks, Government Accountability Office (GAO) was asked to review several aspects of the arms export control system. Specifically, GAO is providing information on (1) changes in the arms export control system since September 2001 and overall trends in arms export licensing, (2) extent of implementation of or revision to initiatives designed to streamline arms export licensing, and (3) extent of coordination on these initiatives between State and arms export enforcement agencies, as well as enforcement efforts. The State Department disagreed with information contained in the report, while the Departments of Defense and Homeland Security generally agreed with the report.
Highlights: http://www.gao.gov/highlights/d05234high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−234

[Return to top]

Banking and Finance Sector

8.

April 07, IDG News Service — **Indian call center workers charged with Citibank fraud.** Former employees of a call center in Pune, India, were arrested this week on charges of defrauding four account holders in the New York branch of Citibank, a subsidiary of Citigroup, for $300,000, according to a police official in Pune. The three former employees of Mphasis BPO, the business process outsourcing (BPO) operation of Bangalore software and services company Mphasis BFL Group, are charged with collecting and misusing account information from customers they dealt with as part of their work at the call center, according to Sanjay Jadhav, chief of the cybercrime cell of the Pune police. "Either in goodwill or on false pretenses, they also obtained the PINs (personal identification numbers) from these account holders in the course of their work," said Jadhav. The police acted on a complaint from Citibank who in turn were alerted when account holders noticed suspicious transactions in their accounts, Jadhav said. The threat of data theft and misuse is no higher in India than in other countries, including the U.S., according to the National Association of Software and Service Companies (NASSCOM) in Delhi. The organization maintains that Indian outsourcing companies have adequate security systems in place.
Source: http://www.infoworld.com/article/05/04/07/HNcitibankfraud_1. html

9. *April 06, TechWeb News* — **Phishers using e−postcards to trap consumers.** Phishers are disguising e−mails as electronic postcards from family in order to lure consumers to sites that deliver a malicious Trojan horse program to their computers. The latest scheme to commandeer someone's computer to steal passwords, spread spam or attempt some other nefarious act was reported this week by The SANS Institute, a cooperative research and education organization. The e−mail arrives as a postcard−pickup notification with a message that reads, "You have just received a virtual postcard from a family member!" Clicking on the link in the message sends the person to a site that uploads a Trojan that hijacks the computer's mIRC, which is a popular Internet Relay Chat program. Because of the increasing sophistication of phishing attacks, the institute advises computer users to take no chances and refuse to accept nearly anything from the web. "Without knowing the true source of an e−mail, one has to be cautious on accepting just about everything these days," the institute said.
Source: http://www.techweb.com/wire/security/160501543

10. *April 06, Agence France−Presse* — **New Internet scam lures victims with cheap airline fares.** A new kind of Internet scam entices victims with a promise of low−cost airline tickets, in a fraud aimed simply at stealing credit card numbers, an online security firm warned. Panda Software said the scheme may be effective because it does not use e−mail but paid listings when a Web user conducts a search with an Internet search engine such as Google. "The real aim of these Internet pages is not to sell anything, but to get users to enter their credit card details which will then fall into the hands of cyber−crooks," Panda Software said. Panda said the sites, which it did not identify, had been shut down, but warned that others may crop up in their place. The Websites ask customers to enter personal details, including their credit card number. But once the details have been entered, an error page is displayed telling the user that the transaction has been unsuccessful, to prolong the illusion. Panda advised Internet users to rely on established and trusted websites and to investigate any new sites offering unusual bargains.
Source: http://www.bakutoday.net/afps/english/shared/hightech/050406 190049.amy9f371.html

[Return to top]

Transportation Sector

11. *April 07, Boston Globe* — **Border crossings hinder training at Arizona bases.** Marines preparing for combat in Iraq or Afghanistan have lost significant amounts of training time because undocumented immigrants from Mexico have constantly wandered onto a bombing test range in Yuma, AZ. Virtually every Marine squadron headed to Iraq or Afghanistan receives combat training at the Marine Corps Air Station in Yuma, which for nearly 40 miles touches the U.S.−Mexico border in the southwestern corner of Arizona. Since July 2004, the training range has been shut down more than 500 times because of immigrants spotted on the range, causing a loss of more than 1,100 training hours, said Colonel James J. Cooney, the base's commanding officer. Cooney said Marines intercepted more than 1,500 undocumented immigrants on the training range last year and, in the first three months of this year, more than 1,100. Base personnel detain the immigrants and call in Border Patrol agents to pick them up. There is some concern that, besides wandering immigrants, foreign terrorists could cross the Mexican border and infiltrate the Arizona bases to conduct intelligence gathering or commit acts of sabotage. Two other bases in Arizona, one the Army's and another the Air Force's, have experienced similar problems.
Source: http://www.boston.com/news/nation/articles/2005/04/07/border_crossings_hinder_training_at_ariz_bases/

12. *April 07, Associated Press* — **Phoenix airport seeks anti−blast trash cans.** Sky Harbor International Airport in Phoenix, AZ, the sixth−busiest airport in world, is looking for stainless−steel trash cans that can withstand a bomb blast while being able to hold 40 gallons of garbage. The airport is following the lead of several other major airports and is accepting bids from makers of blast−resistant trash cans. Each will likely cost between $1,500 and $3,500. While it has happened in Europe, so far no bombs have gone off from trash cans at U.S. airports. But the Transportation Security Administration doesn't want to take any chances and has identified garbage cans as a risk for concealing explosives.
Source: http://www.usatoday.com/travel/news/2005−04−07−blast−cans_x. htm

[Return to top]

Postal and Shipping Sector

13. *April 07, Business Week* — **Mail and commerce increasingly move to the Internet.** Businesses, which account for 95 percent of the U.S. mail stream, are cutting back on first−class mail. Last year the U.S. Postal Service (USPS) passed a milestone: For the first time, first−class mail shrank in both volume and revenues. The latter fell by $617 million, to $36.4 billion. And since first−class mail has long made up over half of USPS' revenues, fears are growing that it's only a matter of time before total revenues start to shrink. Because of its "universal service" obligation −− it must serve 1.8 million new addresses every year −− USPS has limited room to maneuver. These days just five percent of mail goes from consumer to consumer; increasingly, everything else originates and/or ends at a business. In recent years, for example, Internal Revenue Service tax returns have gone from all paper to mostly digital, and the conversion is accelerating. With the same shift occurring simultaneously for all the nation's

paychecks and credit−card statements, USPS has been shedding one billion to two billion pieces of first−class mail per year since 2000.
Source: http://www.businessweek.com/magazine/content/05_15/b3928015. htm

[Return to top]

Agriculture Sector

14. *April 07, Statesman Journal (OR)* — **Two nurseries have sudden−oak−death fungus.** This year, the Oregon Department of Agriculture has inspected and certified more than 900 nurseries as free of the fungus that causes sudden oak death. However, samples taken from a Marion County wholesale nursery and a Washington County retail garden center tested positive for the Phytophthora ramorum, the fungus that causes sudden oak death. All infected or potentially infected plants will be destroyed at the two locations. Known for harming certain oak−tree species, the disease can also infect about 60 varieties of trees and shrubs. That includes landscaping plants such as rhododendrons and many types of camellias that are valuable to Oregon's $778 million−per−year nursery industry.
Oregon Department of Agriculture Website:
http://www.oregon.gov/ODA/PLANT/sod_free.shtml
Source: http://159.54.226.83/apps/pbcs.dll/article?AID=/20050407/BUSINESS/504070324/1040

15. *April 07, Tennessean* — **Fire may keep dogwood−killing fungus at bay.** In an Appalachian forest of dying dogwoods, researchers have found pockets of the flowering trees thriving in parts of the Great Smoky Mountains National Park that had once burned. The number of dogwood trees had doubled in three research plots that were burned in a 1976 wildfire, while dogwood mortality reached 60 to 94 percent elsewhere in the 520,000−acre park straddling the Tennessee−North Carolina border. The discovery could be a great advance in controlling the deadly exotic fungal disease, dogwood anthracnose, that has spread through the forests of the eastern U.S. since the 1970s. "This suggests that maybe by (prescribed) burning, we may be able to maintain conditions that allow dogwoods to persist," ecologist Mike Jenkins said. "Otherwise, the dogwood is being lost from pretty much every stand in the park." Researchers believe that burning clears away the forest canopy and underbrush that contributes to the dense, moist conditions favored by the fungus, leaving plenty of sunlight and a fresh breeze for dogwood sprouts and seedlings.
Source: http://www.tennessean.com/local/archives/05/03/67933326.shtml?Element_ID=67933326

16. *April 06, Pennsylvania Game Commission* — **Chronic wasting disease not found in Pennsylvania deer samples.** Chronic wasting disease (CWD) was not detected in samples taken from hunter−killed deer during the state's 2004 hunting season, according to Pennsylvania Game Commission Executive Director Vern Ross. Based on a significant increase in the number of deer samples collected for testing, Ross noted that the test results took two additional weeks to complete this year. In 2004, 3,699 hunter−killed deer samples were collected for testing, compared to the 2,003 deer sampled in 2003. Last year's results for CWD also were negative. Results showing that the CWD tests of hunter−killed elk from 2004 were all negative and were announced on March 24.

Source: http://www.pgc.state.pa.us/pgc/cwp/view.asp?Q=163761&A=11

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

17. *April 07, Los Angeles Times* — **Polluted water may hurt wells in Arizona.** Arizona environmental officials are worried that a plume of polluted water under a Pacific Gas & Electric Company (PG&E) facility near Needles, CA, may be threatening drinking water wells on the Arizona side of the Colorado River. Pollution from PG&E's Topock natural gas compressor station in the Mojave Desert has created alarm at the Metropolitan Water District of Southern California, which serves Los Angeles and 25 cities and water agencies, the newspaper said. The Topock plant, which pushes natural gas through a pipeline from Texas to markets in California, sits atop a pocket of at least 108 million gallons of water tainted with hexavalent chromium, a chemical compound that can cause cancer if inhaled as dust or steam. PG&E has offered to pay more than $350,000 for a study of possible groundwater contamination in several communities on the Arizona side of the river.
Source: http://www.azcentral.com/news/articles/0407pollution07.html

18. *April 06, Associated Press* — **Government proposes to move nuclear waste from Colorado River.** The Department of Energy on Wednesday, April 6, proposed to move a huge pile of radioactive waste away from the banks of the Colorado River −− a victory for environmentalists and Western politicians who fear the debris could poison the Southwest's major source of drinking water. The pile −− a mostly open−air heap that sits on bare ground and is surrounded only by a chain−link fence −− covers 130 acres near the town of Moab and consists of about 12 million tons of dirt and other waste from decades of uranium ore processing. It contains toxic chemicals and traces of uranium and other radioactive substances. The Department of Energy said it will recommend in an environmental impact statement that the waste be moved to a closed storage facility about 30 miles to the north, near Crescent Junction. The department said it plans no final decision until it reviews all public comment. The site is the only decommissioned uranium mill overseen by the department that has yet to be cleaned up.
DOE Press Release: http://www.energy.gov/engine/content.do?PUBLIC_ID=17743&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE
Source: http://www.usatoday.com/news/nation/2005−04−06−nuclear−waste_x.htm

[Return to top]

Public Health Sector

19.

April 07, New England Journal of Medicine — **Necrotizing fasciitis caused by community associated methicillin−resistant Staphylococcus aureus.** Necrotizing fasciitis is a life−threatening infection requiring urgent surgical and medical therapy. Staphylococcus aureus has been a very uncommon cause of necrotizing fasciitis, but recently researchers have noted an alarming number of these infections caused by community associated methicillin−resistant S. aureus (MRSA). Researchers reviewed the records of 843 patients whose wound cultures grew MRSA at from January 15, 2003, to April 15, 2004. Among this cohort, 14 were identified as patients presenting from the community with clinical and intraoperative findings of necrotizing fasciitis, necrotizing myositis, or both. The median age of the patients was 46 years, and 71 percent were men. Coexisting conditions or risk factors included current or past injection−drug use (43 percent); previous MRSA infection, diabetes, and chronic hepatitis C (21 percent each); and cancer and HIV infection (7 percent each). Four patients (29 percent) had no serious coexisting conditions or risk factors. Wound cultures were monomicrobial for MRSA in 86 percent, and 40 percent of patients for whom blood cultures were obtained had positive results. All MRSA isolates belonged to the same genotype. Researchers concluded necrotizing fasciitis caused by community−associated MRSA is an emerging clinical entity.
MRSA information: http://www.cdc.gov/ncidod/hip/ARESIST/ca_mrsa.htm
Source: http://content.nejm.org/cgi/content/short/352/14/1445

20. *April 07, Trentonian (NJ)* — **Hospitals overwhelmed during mock attack.** Some Mercer County, NJ, hospitals were overrun with plague−infected "patients" Wednesday, April 6, and had trouble coping with staffing shortages when a mock bioterrorism attack reached Trenton, officials said. Measures put in place to protect New Jersey residents actually prevented one hospital from operating efficiently. The exercise, called TOPOFF 3, is the last of three congressionally−ordered drills designed to expose and correct flaws in the nation's ability to respond to a widespread biological disaster. As part of the exercise, all state borders were closed to try to contain the plague and schools were shut down so they could be used as antibiotic distribution sites. But those measures led to problems at Capital Health, said Rick Butler, director of emergency medical and trauma for Capital Health System. "They closed the borders of New Jersey and we have a large population that works at the hospital who are from Pennsylvania. What we had to do was coordinate getting those people here with state police, which can be time consuming," Butler said. "And with schools closing, large numbers of parents needed to make arrangements for their kids or stay home. Once that happens, a limited number of people are taking care of patients and services at the hospital."
Source: http://www.zwire.com/site/news.cfm?newsid=14300285&BRD=1697&PAG=461&dept_id=44551&rfi=6

21. *April 06, University of Adelaide (Australia)* — **Math student models anthrax outbreak.** Using 'survival analysis techniques' Jessica Kasza, who is in her Honors year at the University of Adelaide, is developing a model that could help world health authorities rapidly identify and manage an anthrax outbreak. Anthrax spreads via spores entering the body through a cut in the skin, or the stomach via eating contaminated meat, or the lungs by inhalation. If identified early it can be effectively treated with antibiotics but because its symptoms are similar to flu, it may be left undiagnosed until too late. Survival analysis techniques were first developed to analyze medical and biological data (e.g. for cancer and AIDS research). The techniques allow researchers to take into account information about the development of a potentially fatal disease from not only the people who die from the disease, but also from those who recover either

through treatment or naturally.
Source: http://www.adelaide.edu.au/news/news4402.html

22. *April 06, Reuters* — **U.S. government focusing on disease spread through air travel.** U.S. government health agencies are strengthening ties to airlines and aviation regulators to guard against the spread of infectious diseases or other deadly agents aboard commercial aircraft, federal officials said on Wednesday, April 6. "With over 1.6 billion passengers traveling worldwide each year on commercial air carriers, there is a real threat that these sometimes deadly diseases can be transmitted around the world in a matter of hours," Rep. John Mica, chairman of the House aviation subcommittee, told a hearing attended by government health and aviation experts. Anne Schuchat, acting director for the U.S. Center for Infectious Diseases, noted a case in 2004 when a traveler died from an acute viral illness contracted in Africa soon after arriving in New Jersey. An investigation identified a number of air and train passengers who may have been at risk for the virus but no one else turned up sick. Schuchat told lawmakers that government health agencies are working harder to try to detect problems overseas before someone boards a flight to the U.S. U.S. airlines are working closely with the Centers for Disease Control and Prevention to expedite information electronically about passengers and crew who may have been exposed to a contagious disease or who are sick.
Source: http://www.reuters.com/newsArticle.jhtml?type=topNews&storyI D=8107771

[Return to top]

Government Sector

23. *April 07, Department of Homeland Security* — **Research and development collaboration and information exchange.** More than 500 research scientists and engineers working in government, the private sector, and the academic community will present their innovative work to make the nation safer at the conference, “Working Together: R&D Partnerships in Homeland Security.” The conference, sponsored by the Department of Homeland Security’s Science and Technology Directorate (S&T), will be held April 27−28, 2005, at the Seaport Hotel and World Trade Center in Boston, MA. The conference features 30 technical and four poster sessions on Research & Development advances to better understand, counter and respond to high−consequence chemical, biological, radiological, nuclear, explosives and cyber terrorist threats.
For information and conference registration, visit
http://www.homelandsecurityresearchconference.org/
Source: http://www.dhs.gov/dhspublic/display?content=4436

[Return to top]

Emergency Services Sector

24. *April 07, The Times and Democrat (SC)* — **New Hazmat team trained and equipped for emergencies.** John Smith, Emergency Services director in Orangeburg County, SC, says the county's new Hazmat unit will enable quicker, safer local response to accidents involving hazardous chemical spills or releases. The 30−member volunteer team is comprised of county

and industrial firefighters and chemical specialists and technicians from local industry who have each undergone up to 100 hours of specialized hazardous material training to be able to assist the Orangeburg County Emergency Services Department in the event of a disaster. The emergency services department worked more than three years to recruit and train the volunteer hazardous materials response team and to acquire equipment valued at more than $100,000 with the help of budgeted county funds and grants, including those most recently acquired from the Department of Homeland Security. Smith said team members will get a chance to put their skills to the test during a statewide Homeland Security training exercise in May. The training is in addition to the periodic training exercises in which team members engage.
Source: http://www.timesanddemocrat.com/articles/2005/04/07/news/doc42549da51c380346222863.txt

25. *April 07, The Daily News (NC)* — **Military and civilians conduct drill at air station.** A drill scheduled for Saturday, April 9, at New River Air Station in North Carolina involving the military and civilian agencies will test force protection and anti−terrorism measures, according to the U.S. Marine Corps. "We are going to have a simulated aircraft crash on the flight line," said air station spokesman Sgt. Wayne Campbell. "It will go up the chain of command and get to the FBI level. It eventually will be found out it's a terrorist attack." The purpose of the exercise is to validate plans, train personnel and enhance preparedness in the event of a terrorist, criminal or natural crisis. Many air station departments are participating in the drill, including military police, airfield rescue and firefighting. Nearby Camp Lejeune Naval Hospital will also participate, along with Onslow County agencies. A similar event is planned for Friday at Cherry Point Air Station in North Carolina. The exercise is being organized by Headquarters Marine Corps.
Source: http://www.jdnews.com/SiteProcessor.cfm?Template=Templates/Staff.cfm&Section=Staff

26. *April 07, Associated Press* — **Officials to review anti−terror drills.** The body count may be fake, but the implications aren't. With a massive anti−terror drill in both New Jersey and Connecticut nearing its conclusion, federal officials were preparing for a thorough review to pinpoint where things went wrong so they can be corrected in the event of a real catastrophe. "There's no doubt we're going to learn some things from this," said Department of Homeland Security Secretary Michael Chertoff, who was in New Jersey on Wednesday, April 6, for an up−close inspection. The five−day TOPOFF 3 drill, which began Monday, involves public officials, law enforcement, first responders and hospitals and health care personnel in New Jersey and Connecticut. The New Jersey portion of the exercise simulates a bioterror attack launched from a sport utility vehicle with a commercial sprayer in Union County. Fatigue among hospital workers and the complex logistics of a massive evacuation effort were two areas identified in the early stages of the exercise as potentially problematic, officials said. In Connecticut, authorities simulated a mustard gas attack. They confirmed nearly 200 mock deaths, more than 4,600 supposed injuries and some missing people. Three mock arrests were made based on FBI warrants.
Source: http://www.mercurynews.com/mld/mercurynews/news/breaking_news/11328256.htm

27. *April 06, Reuters* — **Dutch stage mock terrorist attack.** The Netherlands staged a mock terrorist bomb attack on a rap concert on Wednesday, April 6, to test the readiness of its emergency services to cope with such an event. The exercise was organized in response to the

March 2004 Madrid train bombings, which raised fears of other similar attacks across Europe. Thousands of volunteers took part in the drill at the Amsterdam Arena soccer stadium, some playing injured as smoke billowed from the scene after the mock attack. Up to 2,000 fire, ambulance, police and other officials took part in the exercise. The wounded were treated in and around the ground as emergency helicopters hovered overhead. Wednesday's exercise, codenamed "Bonfire", will cost around $1.29 million.
Source: http://www.alertnet.org/thenews/newsdesk/L0661769.htm

28. *April 06, Hudson Valley News (NY)* — **New Yorkers concerned about preparedness for future terror attacks.** With the largest anti−terror drill underway in selected places around the country, 68 percent of New York City residents do not think their community has an adequate emergency response plan in the event of a future terror attack. Eleven percent are unsure about their community's preparedness and 21 percent do think their community has a plan in place to deal with a terror emergency. The findings are the results of the latest poll conducted by the Marist Institute for Public Opinion in Poughkeepsie. Thirty−two percent of New York City residents have confidence in the government to protect the subways and bridges in the New York City area from future terror attacks. There is also concern about the ability to protect the area's nuclear power facilities, the water supplied to communities, Grand Central Station, and the airports. Fifty−three percent of New Yorkers do have confidence that an attack against a specific historical site such as the Empire State Building or the Statue of Liberty would be thwarted. Thirty−five percent of New York City's residents have some semblance of an emergency plan in the event of a terrorist attack, the poll said.
Poll: http://www.maristpoll.marist.edu/nycpolls/TR050405.htm
Source: http://www.midhudsonnews.com/News/MarPoll_terror−06Apr05.htm

[Return to top]

Information Technology and Telecommunications Sector

29. *April 07, SC Magazine (UK)* — **German police hard drive containing confidential information sold on eBay.** A hard drive full of confidential police data has been sold on eBay, for only $25. Germany's Spiegel newspaper reported earlier this week that the 20GB hard drive contained a raft of information about Brandenburg police, including details of political security situations. "This week's exposure of leaked and highly critical information from the Brandenburg police in Germany reinforces how important it is to never let mobile devices or hard drives leave the office without being adequately protected with encryption and strong password protection −− even after they have been discarded," said Peter Larsson, CEO of mobile technology company Pointsec. The drive was eventually bought by a student from Potsdam who alerted police once he realized what it contained.
Source: http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=023c9f0f−7295−49c5−b349−847df8e174b2&newsType=La test%20News

30. *April 07, Government Accountability Office* — **GAO−05−483T: Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements (Testimony).** For many years, the Government Accountability Office (GAO) has reported that poor information security is a widespread problem that has potentially devastating consequences. This testimony reports on the federal government's progress and challenges in

implementing the Federal Information Security Management Act of 2002 (FISMA) as reported by the Office of Management and Budget (OMB), the agencies, and Inspectors General (IGs). In its fiscal year 2004 report to the Congress, OMB reports significant strides in addressing long−standing problems, but at the same time, cites challenging weaknesses that remain. Fiscal year 2004 data reported by 24 major agencies generally show increasing numbers of systems meeting key statutory information security requirements compared with fiscal year 2003. Nevertheless, challenges remain. For example, only seven agencies reported that they had tested contingency plans for 90 to 100 percent of their systems, and six of the remaining 17 agencies reported that they had tested plans for less than 50 percent of their systems. Opportunities also exist to improve the usefulness of the annual FISMA reporting process. In addition, a commonly accepted framework for the annual FISMA mandated reviews conducted by the IGs could help ensure the consistency and usefulness of their evaluations.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−483T

31. *April 06, FrSIRT* — **Cisco IOS IKE Xauth authentication bypass vulnerabilities.** Two vulnerabilities were identified in Cisco IOS, which may be exploited by remote attackers to gain unauthorized access to the network resources. The first flaw resides in the Easy VPN Server XAUTH feature which fails to handle certain malformed packets (port 500/udp). The second vulnerability exists where the ISAKMP profile is assigned but the attributes that are configured in the ISAKMP profile are not processed.
Original advisory and solution:
http://www.cisco.com/en/US/products/products_security_advisory09186a008042d519.shtml#software
Source: http://www.frsirt.com/english/advisories/2005/0321

32. *April 06, InformationWeek* — **Committee to inform DHS on privacy issues.** A new group of public− and private−sector leaders in academia, business, and technology met Wednesday, April 6, in Washington, DC, to help the Department of Homeland Security (DHS) gain a greater understanding of how IT can be used to fight terrorism without exposing personal data to theft or abuse. The department's Data Privacy and Integrity Advisory Committee launched with a statement of mission and the selection of its inaugural chairman and vice chairwoman. Paul Rosenzweig, the committee's new chairman and a senior legal research fellow at the Heritage Foundation, said that the committee's greatest challenge will be helping the department as a whole focus on preserving individual freedoms while tightening security, and doing this in a public way. The committee will serve to inform DHS about privacy concerns related to all of the department's various agencies and directorates, which protect the nation's borders, waterways, and critical infrastructure.
DHS Privacy Office: http://www.dhs.gov/privacy
Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=160501384

33. *April 06, InformationWeek* — **Businesses suffer more downtime from viruses.** Damage to business IT systems caused by viruses continues to grow, and businesses are getting hit by more viruses, according to a new survey. IT systems were hit with 50% more viruses in 2004 than they were in 2003, reaching 392 incidents per 1,000 machines, according to a survey of 300 companies and government agencies sponsored by McAfee, Microsoft, Trend Micro, and other vendors, and conducted by ICSA Labs, a division of Cybertrust Inc. The Virus Prevalence Survey indicates that when 25 or more PCs or servers are infected, system downtime increased

by 12% in 2004 compared with a year earlier. The amount of time it took in 2004 to recover from the infections increased by seven person days, year over year, and the actual costs of recovery averaged $130,000. Both of those figures were 25% higher than in 2003.
Survey details: http://www.cybertrust.com/pr_events/2005/20050405.html
Source: http://www.informationweek.com/story/showArticle.jhtml;jsessionid=JEJIDQB3K21CEQSNDBGCKHSCJUMEKJVN?articleID=160501452

34. *April 05, Federal Times* — **Group aims to boost federal information security.** A group of government and industry executives will meet for the first time this month to map out a strategy for improving the government's information security. The CISO Exchange is comprised of five chief information security officers from various federal agencies, one federal chief security officer, and two executives from information technology companies. It is a privately funded working group that will hold quarterly educational meetings and produce an annual report on the government's information technology security policies and operational issues. The exchange was announced in February by the federal Chief Information Officers Council and Representative Tom Davis from Virginia, chairman of the House Government Reform Committee. They announced the exchange as a way to boost security through educational meetings between chief information security officers and others in government and private industry. The group also will work with the Government Accountability Office and inspector general offices. At least 50 companies have inquired about joining the exchange, said Stephen O'Keeffe, of O'Keeffe & Company, the company managing the meetings. The two fellows on the exchange so far paid $75,000 apiece, he said.
Source: http://www.federaltimes.com/index2.php?S=766429

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

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

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 6346 (gnutella−svc), 135 (epmap), 20525 (−−−), 1433 (ms−sql−s), 139 (netbios−ssn), 1026 (−−−), 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

35. *April 07, News.com.au (Australia)* — **Australian restaurant blown apart by roach bombs.** A combination of 36 cockroach bombs and an oven pilot light blew apart a Thai restaurant in Perth, Australia, injuring three men, two seriously. A massive explosion rocked suburban Duncraig on Thursday, April 7, after chemicals released during the night's do−it−yourself fumigation ignited, blowing out the back wall and lifting the roof off the Tamarind restaurant. The blast caused an estimated $500,000 damage, fire authorities said. The restaurant owner and two staff members had closed the premises to set off 36 insect−control bombs throughout the building. Eight bombs would have been enough, West Australian police and fire and emergency personnel said. Investigators believed a pilot light in one of the restaurant's ovens ignited the huge amount of chemicals released by the bombs to kill insects such as fleas and cockroaches. The three men, who had reached the restaurant's front door when the explosion occurred, were hospitalized with burns. John McMillan, manager of the state fire investigations unit, said the pressure wave from the blast was powerful enough to lift the roof off the building.
Source: http://www.news.com.au/story/0,10117,12782848−29277,00.html

36. *April 06, Government Accountability Office* — **GAO−05−516T: Kennedy Center: Stronger Oversight of Fire Safety Issues, Construction Projects, and Financial Management Needed (Testimony).** Since fiscal year 1995, the John F. Kennedy Center for the Performing Arts (Kennedy Center) has received nearly $203 million in federal funds to complete capital projects and intends to request an additional $43 million in appropriations through fiscal year 2008. The Kennedy Center's Comprehensive Building Plan identifies these capital projects as necessary to renovate the Center and to meet or exceed relevant life safety and disabled access regulations. The Government Accountability Office (GAO) was asked to examine (1) the progress the Center has made in completing key capital projects within estimated costs and the information it has communicated about this progress to key stakeholders; and (2) the status of the Center's plans to address fire life safety and disabled access requirements. GAO made recommendations to the Chairman of the Kennedy Center Board of Trustees including increasing oversight and better complying with fire safety code. The Kennedy Center agreed that more oversight would be useful, but it is unsure what the best mechanism would be for providing such oversight. Furthermore, the Kennedy Center believes that it is in compliance with fire code, but has agreed to seek third party review of its approach in addressing certain fire code deficiencies. Highlights: http://www.gao.gov/highlights/d05516thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−516T

[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