# Department of Homeland Security
# IAIP Directorate
# Daily Open Source Infrastructure Report
# for 07 April 2005

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

**Daily Highlights**

- The Financial Services Sector Coordinating Council has announced a comprehensive action agenda identifying the five most critical issues for protecting the nation's financial infrastructure in 2005. (See item 7)
- The Washington Post reports U.S. District Judge Emmet G. Sullivan has proposed a 30−day cooling−off period for settlement talks between the Washington, DC government and CSX Transportation over rail shipments of hazardous materials through the city. (See item 9)
- 1010 WINS reports that as the nation's largest−ever terrorism drill, TOPOFF 3, entered its third day, officials said there have been some communications problems, but added the drill has been a success overall. (See item 26)

**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 06, L.A. Times* — **Probe of possibly fabricated reports stalls nuclear waste repository.** The Department of Energy will not consider seeking a license for the proposed nuclear waste repository at Yucca Mountain in Nevada until investigations into possible falsification of water−safety surveys are complete, officials said Tuesday, April 5. "We have not made a final decision yet as to when or whether to file those [licensing] documents, and some of that will be

based on this investigation," Theodore Garrish, the department's deputy director for civilian radioactive waste management, told the House government reform subcommittee on federal workforce and agency organization. Last month, the Energy and Interior departments, along with the FBI, began criminal investigations to determine whether e−mails among scientists proved that those reports were fabricated to keep the project going. The data in question indicated that the water levels at the site would not corrode storage tanks for 77,000 metric tons of nuclear waste for 10,000 years, preventing groundwater contamination. The project to provide a single storage place for the country's nuclear waste from power plants and bomb production, now kept at 131 sites throughout the country, is 14 years behind schedule and could cost as much as $100 billion.
Source: http://www.latimes.com/news/nationworld/nation/la−na−yucca6apr06,0,7514014.story?coll=la−home−nation

2. *April 06, The National Academies* — **Study says spent fuel at some nuclear power plants potentially at risk from terrorist attacks.** Spent nuclear fuel stored in pools at some of the nation's 103 operating commercial nuclear reactors may be at risk from terrorist attacks, says a new report from a committee of the National Academies' Board on Radioactive Waste Management. The report calls on the Nuclear Regulatory Commission (NRC) to conduct additional analyses to obtain a better understanding of potential risks and to ensure that power−plant operators take prompt and effective measures to reduce the possible consequences of such attacks. Because potential threats may differ according to a specific plant's design, the committee recommended that plant−by−plant vulnerability analyses be performed. These conclusions were based on a detailed review of security analyses performed by the NRC, Department of Homeland Security, the nuclear power industry, and independent experts. Congress requested the study following conflicting claims in the media about the safety and security of spent fuel in storage at commercial nuclear power plants, including the risks that spent fuel might be used to construct a radiological dispersal device, or "dirty bomb." The committee concluded the likelihood that terrorists could steal enough spent nuclear fuel from a power plant for use in a dirty bomb is small, given existing security measures. Nevertheless, the NRC should review and upgrade where necessary its security requirements for protecting those spent fuel rods not contained in fuel assemblies from theft by knowledgeable insiders.
Source: http://www4.nationalacademies.org/news.nsf/isbn/0309096472?O penDocument

3. *April 05, Reuters* — **Lawmaker wants list of companies exporting U.S. oil.** With gasoline and crude oil prices at record highs, a U.S. lawmaker wants the Department of Commerce to release the names of American companies that are shipping U.S. petroleum products to other countries. Senator Ron Wyden (D−OR) says information on the 268 million barrels of U.S. petroleum products exported in 2004 is needed as Congress considers a broad energy bill. The United States consumes about 20.8 million barrels of petroleum a day, with imports accounting for about 58 percent of supply. However, about one million barrels of U.S. oil petroleum products are exported daily.
Source: http://channels.netscape.com/ns/news/story.jsp?id=2005040512350002903521&dt=20050405123500&w=RTR&coview

4. *April 05, Associated Press* — **Venezuela official comments on OPEC.** The Organization of Petroleum Exporting Countries (OPEC) is running out of spare production capacity, Venezuelan Oil Minister Rafael Ramirez said Tuesday, April 5. "OPEC's production capacity is

reaching its limit," Ramirez told reporters, adding that it is too early for OPEC to decide on a possible half−million barrel per day production increase. Ramirez argued that geopolitical tension in the Middle East has contributed more to recent oil price rises than have any supply problems. Venezuela is the world's fifth largest oil exporter and one of the top price hawks within OPEC, which produces nearly 40 percent of the world's oil supply.
Source: http://biz.yahoo.com/ap/050405/venezuela_opec.html?.v=1

[Return to top]

## Chemical Industry and Hazardous Materials Sector

5. *April 06, Niles Daily Star (MI)* — **Hazmat called to construction site.** A 55−gallon barrel containing an unknown liquid was found buried at a dental office that is under construction in Niles, MI, on Tuesday, April 5. Concerned that the liquid in the barrel might be hazardous, the construction−site supervisor placed a call to the health department who notified the police dispatcher who, in turn, alerted the fire department. According to Lt. Bill McAllister of the city fire department, when the Niles City Fire Department receives notice from the police dispatcher of possible chemical contamination, a dispatch tone is issued for the city's fire department. A request is also sent to the Niles Township Fire Department's hazardous materials personnel. In turn, the Niles City Police notify their own hazardous materials team, and the three departments work together to investigate the situation. Protocol also requires that the Berrien County hazardous materials team be notified. They offer additional resources and, if needed, join the other departments either on site or at the fire station. On orders from construction−site supervisor, all the workers were sent home until the situation could be evaluated. The fire department is currently testing the contents of the barrel and will issue a report at a later date.
Source: http://www.leaderpub.com/articles/2005/04/06/news/niles_star /ndnews3.txt

[Return to top]

## Defense Industrial Base Sector

Nothing to report.
[Return to top]

## Banking and Finance Sector

6. *April 06, Computing* — **UK government and banks to improve online authentication.** The UK government is to work with the banking industry to establish the sector as a pioneer of online authentication. As part of a strategy launched last week to promote public access to technology, the government aims to create a framework to increase confidence in the identity of online users, both in transactions and social contact. The "Connecting the UK" strategy includes a range of measures to increase the role of IT in education, boost the development and adoption of online government services, and improve Internet safety. The government has already revealed plans to work with the private sector to determine how to use ID cards for a range of commercial transactions.
Strategy: http://www.strategy.gov.uk/

Source: http://www.computing.co.uk/news/1162335

7. *April 05, Financial Services Sector Coordinating Council* — **Financial group identifies critical concerns for financial infrastructure protection.** The Financial Services Sector Coordinating Council (FSSCC) announced on Tuesday, April 5, it has issued a comprehensive action agenda identifying the five most critical issues for protecting the nation's financial infrastructure in 2005. In the report, Protecting the U.S. Critical Financial Infrastructure: An Agenda for 2005, the five critical issues identified are: Strengthening the financial system's core components by implementing the rigorous standards of the Interagency Sound Practices paper; Creating a more structured and coordinated approach to testing efforts; Promoting industry−wide standards for business continuity and resilience; Expanding the membership of the Financial Services Information Sharing and Analysis Center (FS/ISAC), and outreach and education efforts; and Identifying and testing critical interdependencies between financial services and other sectors. "To one extent or another, all private sector organizations are working to strengthen their backup operations, test telecommunications networks, and simulate emergency events and crisis response," said Donald F. Donahue, Sector Coordinator and Chairman of the FSSCC. "This 2005 action agenda further enhances these efforts by focusing energy and attention on the vital continuing issues, at both a regional and a national level."
Report: http://www.fsscc.org/reports/FSSCC_2005_Agenda.pdf
Interagency Sound Practices paper:
http://www.federalreserve.gov/boarddocs/SRLETTERS/2003/SR030 9a1.pdf
Source: http://www.fsscc.org/news/2005_agenda.html

8. *April 04, The Standard (UK)* — **More sophisticated cyber crime costs UK billions.** As cybercriminals grow in sophistication and organized crime becomes increasingly involved in the mix, the cost of cybercrime to UK business continues to grow, resulting in billions lost in down time, systems damage and client loss, according to a report released Tuesday, April 5, by the National Hi−Tech Crime Unit (NHTCU). As of last year, the estimated minimum cost of the impact of high−tech crime on companies based in the UK with more than 1,000 employees was US$4.61 billion the NHTCU said. In the survey of 200 large and medium−size companies, 89 percent said that they had experienced some form of high−tech crime in 2004; of those, 90 percent suffered from unauthorized access to, or penetration of, their company systems, while 89 percent suffered theft of information or data, the NHTCU said. Security breaches occurred from outside and, more often, from within a company's system. The Director General of the National Crime Squad, Trevor Pearce, estimated that in 2004, nine out of 10 companies in the UK suffered some sort of cybercrime, reiterating the study's findings, and that the growing spread of that crime was having far reaching effects.
Study: http://www.nhtcu.org/media/documents/publications/NOP_05.pdf
Source: http://www.thestandard.com/internetnews/001188.php

[Return to top]

## Transportation Sector

9. *April 06, Washington Post* — **Cooling−off period proposed in Hazmat rail dispute.** A federal judge said on Tuesday, April 5, that he wants to broker a compromise between the Washington, DC government and CSX Transportation in the dispute over rail shipments of

hazardous materials through the city. U.S. District Judge Emmet G. Sullivan proposed a 30−day cooling−off period for settlement talks. Under the judge's plan, the city would delay enforcing a looming ban on hazardous rail shipments and CSX would not move the cargo on rails in the District during the 30 days. The case stems from a new District law that prohibits the shipment of hazardous materials on the 37 miles of rail lines in the city. City leaders said the ban was necessary because the nation's capital is a probable target for terrorist attacks, and an attack on a rail car loaded with propane or chlorine could release a poisonous cloud capable of killing 100,000 residents. CSX filed a lawsuit to overturn the ban, saying only that the federal government has the power to regulate rail security and that such bans could cripple the nation's rail transportation. The Department of Justice agrees with CSX.
Source: http://www.washingtonpost.com/wp−dyn/articles/A28291−2005Apr 5.html?sub=AR

**10.** *April 06, Associated Press* — **Man charged after allegedly disrupting flight.** A criminal complaint was filed Tuesday, April 5, in federal court against a California man accused of disrupting a United Airlines flight from Kauai to San Francisco. Raymond Cassidy, 31, was arrested Monday after his belligerence caused the pilot of Flight 74 to turn the plane back and land in Honolulu, federal prosecutors said. Cassidy was charged with knowingly interfering with the duties of an airline flight crew, a charge that carries a maximum penalty of 20 years in prison, they said. Cassidy became disruptive after he was refused alcohol, officials said. He became argumentative, refused to sit down, removed his shirt and violently pushed away the hand of female flight attendant, making her fearful of his behavior, they said.
Source: http://www.usatoday.com/travel/flights/2005−04−06−unruly−fli er_x.htm

**11.** *April 06, Associated Press* — **Border group spends night without incident.** Clusters of citizens who volunteered to watch for illegal immigrants and smugglers along a swath of the Mexican border passed their first night of full patrols without incident, authorities said Tuesday, April 5. Volunteers for the Minuteman Project had spent Monday expanding their line southeast of this border community. They gathered in groups of three or four spaced out about every quarter mile. Some sat in lawn chairs, others stood scanning the desert with binoculars. The volunteers, many of whom were recruited over the Internet, plan to watch the border in shifts 24 hours a day during April and report any illegal activity to federal agents. Border patrol officials said the volunteers have been peaceful but have still been disrupting U.S. Border Patrol operations by unwittingly tripping sensors that alert agents to possible intruders. The idea, according to project organizers, is partly to draw attention to problems on the Arizona−Mexico border, considered the most vulnerable stretch of the 2,000−mile southern border. Of the 1.1 million illegal immigrants caught by the Border Patrol last year, 51 percent crossed into the country at Arizona.
Minuteman Project Website: http://www.minutemanproject.com
Source: http://story.news.yahoo.com/news?tmpl=story&cid=519&ncid=718 &e=10&u=/ap/20050405/ap_on_re_us/border_volunteers

**12.** *April 06, Reuters* — **A plan to save airlines billions.** Cutting−edge technology that would lower costs for airlines and make travel easier for passengers is exactly what the ailing airline industry needs, International Air Transport Association (IATA) chief Giovanni Bisignani said at the Airfinance conference in New York, on Monday, April 4. Bisignani offered a bleak outlook for the airline industry −− forecasting it would lose $5.5 billion in 2005 −− but said the implementation and standardization of new technology should save airlines close to $10 billion

a year. The IATA, an industry group that coordinates aviation rules and standards, calls its new plan "Simplifying the Business," and is made up of four main parts. The first part, which would save the industry $3 billion a year, eliminates paper tickets by the end of 2007. The second and third parts will standardize electronic boarding passes and self−service kiosks, both of which would allow usage over multiple airlines. The fourth part −− and the one that will likely take the longest and cost the most −− revolves around standardizing the process of switching baggage labels to wireless tags from printed bar codes, based on radio−frequency identification technology. Of the 1.5 billion bags carried by commercial flights each year, about 0.7% get lost or misplaced. Dealing with the process costs an airline about $100 per bag, Giovanni said.
Source: http://www.usatoday.com/travel/flights/2005−04−05−airlines−i ata_x.htm

**13.** *April 06, Marin Independent Journal (CA)* — **FBI probes Bay Bridge welding.** The new San Francisco Bay Bridge is riddled with defective welds, 15 welders told the reported in a nine−month investigation −− allegations that could lead to criminal fraud charges. The welders' claims have prompted an FBI investigation. In the worst case, the federal probe could lead to tearing apart the new bridge to see if it is structurally sound or needs to be rebuilt. The FBI began investigating allegations in February that welders were "encouraged or instructed to save time by producing substandard welds," said FBI Special Agent in Charge Mark Mershon of the bureau's San Francisco division. The new span is the largest public works project in California history. The state is spending $6.2 billion to replace the vulnerable 70−year−old bridge between Oakland and Yerba Buena Island with one that will stay open after the most violent earthquakes. Every day, 282,000 cars cross the bridge. The allegations involve the first part of the new bridge, a $1.5 billion skyway held up by 160 steel legs. Each leg is riddled with weak welds, because some supervisors ordered welders to hide defects, workers said. Several welders in interviews estimated one−third of the 5,280 welds in these legs, or piles, may be substandard. Almost all are now encased in concrete.
Source: http://www.marinij.com/Stories/0,1413,234~26642~2801705,00.h tml

**14.** *April 05, GovExec* — **Border agency nearly "overwhelmed," chief says.** Bureau of Customs and Border Protection (CBP) Commissioner Robert Bonner acknowledged in an interview Monday, April 4, that the Border Patrol is "almost ... being overwhelmed" by illegal immigration. The Border Patrol caught about 1.1 million illegal immigrants in fiscal 2004, but an estimated 10 million illegal aliens are in the country. The strategy consists of five main objectives: establish substantial probability of apprehending terrorists and their weapons as they attempt to enter illegally between the ports of entry; deter illegal entries through improved enforcement; detect, apprehend and deter smugglers of humans, drugs and other contraband; leverage "smart border" technology to multiply the effect of enforcement personnel; and reduce crime in border communities to improve the quality of life and economic vitality of targeted areas. The plan acknowledges that many areas along the Southwest border are not yet under operational control, adding that daily attempts to cross the border by thousands of illegal aliens from countries around the globe continue to present a threat to U.S. national security. "... an ever−present threat exists from the potential for terrorists to employ the same smuggling and transportation networks, infrastructure, drop houses, and other support and then use these masses of illegal aliens as 'cover' for a successful cross−border penetration."
Strategy: http://www.cbp.gov/linkhandler/cgov/border_security/border_p atrol/national_bp_strategy.ctt/national_bp_strategy.pdf
Source: http://www.govexec.com/dailyfed/0405/040505c1.htm

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

15. *April 06, Associated Press* — **Department Environmental Conservation will kill deer to stop spreading of chronic wasting disease.** New York state officials will begin killing wild deer in central New York to see if chronic wasting disease (CWD) has spread from captive herds. Two captive deer in Oneida County tested positive last week for the fatal neurological illness. State Department of Environmental Conservation officials announced they will kill 420 wild deer in the county starting next week. Brain tissue will be collected and tested to see if the disease has spread to deer in the wild. CWD has been detected in wild and captive deer and elk populations in 12 states in the West and Midwest. Animals in the two captive herds with confirmed positives have been killed and will be tested for CWD.
Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−deerdisease0406apr06,0,3443772.story?coll=ny−region−apnewyork

16. *April 05, Agriculture Online* — **Monsanto completes acquisition of Emergent's cotton business.** The Monsanto Company has completed the acquisition of Emergent Genetics' cotton business. Emergent, which is the third largest cottonseed company in the U.S., will be integrated into Monsanto's existing commercial operations. Emergent's Stoneville and NexGen brands account for about 12 percent of the U.S. cottonseed market. The deal was first announced in mid−February. At that time it was valued at $300 million.
Source: http://www.agriculture.com/ag/story.jhtml?storyid=/templatedata/ag/story/data/agNews_050405crCOTTON.xml&catref=ag1001

[Return to top]

## Food Sector

17. *April 05, Food Safety and Inspection Service* — **Sausage products recalled.** Winter Sausage Manufacturing, an East Point, MI, firm, is voluntarily recalling approximately 5,117 pounds of sausage that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday, April 5. The products were distributed to retail stores in Michigan. The problem was discovered through FSIS microbial 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_016_2005_Relase/index.asp

18.

*April 05, Food Safety and Inspection Service* — **Chicken sandwiches recalled.** LSG Sky Chefs, Inc., an Orlando, FL, firm, is voluntarily recalling approximately 3,316 pounds of chicken wrap sandwiches that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday, April 5. The chicken wrap sandwiches were distributed to convenience stores in Florida. The problem was discovered through company 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_015_2005_Relea se/index.asp

**19.** *April 04, Food and drug Administration* — **Salad recalled.** Mid Atlantic, Inc., of New York, NY, is recalling store−made Pulpo Salad due to Listeria contamination. The product was packed from bulk and sold in an uncoded, circular, clear plastic container weighed at time of sale. The Pulpo Salad was sold in the New York City area. Listeria is a common organism found in nature. It can cause serious complications for pregnant women, such as stillbirth. Other problems can manifest in people with compromised immune systems. Listeria can also cause serious flu−like symptoms in healthy individuals. The problem was discovered after routine sampling by "New York State Department of Agriculture and Markets Food Inspectors and subsequent analysis of the product by food laboratory personnel, found the product to be positive for Listeria monocytogenes.
Source: http://www.fda.gov/oc/po/firmrecalls/midatlantic04_05.html

[Return to top]

## Water Sector

Nothing to report.
[Return to top]

## Public Health Sector

**20.** *April 06, Reuters* — **Bird flu strains could combine.** Two strains of bird flu in Asia may combine to create a highly lethal and easily transmissible virus, a UN health official warned Wednesday, April 6. The UN Food and Agriculture Organization on Tuesday, April 5, confirmed that birds in North Korea were infected with the H7 bird flu strain that sickened nearly 90 people and killed one in the Netherlands two years ago. It is distinct from the H5N1 strain that has decimated poultry populations across Asia since December 2003 and killed at least 50 people in Vietnam, Thailand, and Cambodia. Both strains can jump from birds to humans but only the H7 virus has been shown to spread from person to person, raising concern that it could unite with the deadlier H5N1 strain and cause a global pandemic.
Source: http://abcnews.go.com/International/wireStory?id=645519

**21.** *April 06, Reuters* — **Bird flu kills Vietnamese girl, Asia toll now 50.** A 10−year−old girl has become Vietnam's 36th bird flu victim, a state−run newspaper on Wednesday, April 6, quoted researchers as saying. The teenager, who died on March 27 at a Hanoi hospital, lived on the capital's outskirts in Long Bien, the Hanoi Moi Tin Chieu daily quoted the National Institute of

Hygiene and Epidemiology as saying. In January the Agriculture Ministry said bird flu was detected at two farms in Long Bien district and 1,000 chickens and ducks there had been slaughtered. The latest fatality took to 50 Asia's number of deaths from the H5N1 influenza virus since it first hit the region in 2003.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=8098944

**22.** *April 06, Orlando Sentinel (FL)* — **Biomedical researcher accused of theft.** A University of Central Florida (UCF) visiting scientist relinquished his passport Tuesday, April 5, after spending nearly two weeks in jail on charges he stole vials containing DNA pieces from a tuberculosis (TB) organism and computer discs containing research materials, authorities said. Singh Laxman Meena, 33, working at UCF's Biomolecular Science Center on a fellowship, was researching TB genes to find out their function for the past year, said Pappachan E. Kolattukudy, the center's director. Authorities said Meena stole eight vials of cloned DNA pieces from the TB organism that could be used to develop drugs to fight TB. They said he also took two computer discs that contained information from the study. He was scheduled to return to India days after his arrest, authorities said. The TB organism is considered by the U.S. government as a potential weapon for bioterrorism, authorities said. Kolattukudy said the vials in question did not contain anything dangerous.
Source: http://www.orlandosentinel.com/news/orl−locprofessor06040605 apr06,1,1585556.story?coll=orl−news−headlines&ctrack=1&cset= true

**23.** *April 05, United Press International* — **France has two more mad cow cases in humans.** Two new cases of human mad cow disease were detected in France, raising the total number of cases in that country to 11, health officials said. The country's Institut de Veille Sanitaire said in a statement the two patients were not known to be blood donors. Human mad cow disease, known formally as variant Creutzfeldt Jakob disease (vCJD) can be transmitted via the blood. Humans can contract the incurable, fatal disease by consuming beef products infected with the mad cow pathogen. More than 160 instances of vCJD have been identified around the world, with the bulk −− 154 cases −− occurring in the United Kingdom, where there a massive outbreak of mad cow disease began in the 1980s.
Source: http://www.sciencedaily.com/upi/index.php?feed=Science&artic le=UPI−1−20050405−12222300−bc−france−madcow.xml

[Return to top]

## Government Sector

**24.** *April 04, Associated Press* — **War on terror creates demand for super−secure offices.** Due to the war on terrorism, offices designed to safeguard data, process classified information, and keep conversations private are being leased by federal defense and intelligence contractors in the national capital region as fast as developers can build them, authorities say. Some rooms have walls lined with steel or made of eight−inch−thick concrete to meet federal requirements. Other security standards mandate elaborate alarm systems, sound−masking technology and vent grates to block intruders. The government calls such spaces Sensitive Compartmented Information Facilities, or SCIFs. Developers are building or planning more of them near the National Security Agency headquarters south of Baltimore, and at other locations in the region including the Army biodefense laboratories in Frederick and the former Fort Ritchie Army base

in the Blue Ridge Mountains, 70 miles northwest of Washington. Not since the Cold War has demand for super−secure office space been so strong, said Dennis J. Lane, of Ryan Commercial Real Estate Services. "In the post−9/11 world, it came back with a vengeance," he said.
Source: http://www.securityinfowatch.com/article/article.jsp?siteSec tion=306&id=3553

[Return to top]

## Emergency Services Sector

**25.** *April 06, Asbury Park Press (NJ)* — **Bioterror drill tests first responders.** The second day of a mock terrorist attack spread to Monmouth County, NJ, Tuesday, April 5, as local police and county health officials began combating a "lethal plague" that sent dozens of "patients" to area hospitals. By afternoon, Monmouth County health officials had turned parts of Brookdale Community College in Middletown, NJ, into a drug distribution center, where 400 emergency workers and officials prepared to fight the spreading biological terrorist attack. The increasingly complex exercise is part of the weeklong TOPOFF 3, a terrorism response drill directed by the U.S. Department of Homeland Security, which also involves agencies in Connecticut, Britain and Canada. The weeklong drill began Monday in Middlesex and Union counties in New Jersey with an investigation of a black sport−utility vehicle suspected of releasing an aerosolized form of the deadly pneumonic plague. The drill has been designed to find weak points in the state's planning for a terrorist attack.
Fact Sheet: TOPOFF 3 New Jersey Venue:
http://www.dhs.gov/dhspublic/display?content=4411
Fact Sheet: TOPOFF 3 Background, Biological Agents:
http://www.dhs.gov/dhspublic/display?content=4408
Source: http://www.app.com/apps/pbcs.dll/article?AID=/20050406/NEWS/504060429/1001/NEWS02

**26.** *April 06, 1010 WINS (CT)* — **Terror drill at Connecticut nuke plant.** A specialized group of soldiers was set to provide security at the Millstone nuclear power plant complex in Waterford, CT, on Wednesday, April 6, as the nation's largest−ever terrorism drill, TOPOFF 3, entered its third day. Officials operating the drill made it look like a mustard gas attack. They confirmed nearly 200 mock deaths, more than 4,600 supposed injuries and some missing people. The Pentagon was to deploy the quick reaction force from Fort Bragg, NC, after a briefing at the Camp Rell National Guard facility in Niantic, CT. Gov. M. Jodi Rell praised the state's response on Tuesday, but said there were times when she wanted information faster than she could get it. Officials said there have been some communications problems, but added the drill has been a success overall. TOPOFF is the first congressionally mandated drill since the National Response Plan went into effect. Officials will carefully review results in the coming week and make some changes as necessary.
Fact Sheet: TOPOFF 3 Connecticut Venue:
http://www.dhs.gov/dhspublic/display?content=4409
Fact Sheet: TOPOFF 3 Background, Chemical Agents:
http://www.dhs.gov/dhspublic/display?content=4405
National Response Plan: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_05 66.xml
Source: http://1010wins.com/topstories/local_story_096071725.html

27. *April 05, Palo Alto Weekly (CA)* — **City to debut new emergency notification upgrades.** Starting in May, Palo Alto, CA, will debut some upgrades to the community−notification system. With the new system, residents will be phoned with a recorded message during a crisis. The city's current automated phone system can make about 2,500 calls an hour. But Palo Alto has some 26,000 households, and a number of those have more than one phone line. At the current rate, it would take at least a half−day to alert the whole city of an emergency situation. In about six weeks, the city is expected to contract with a Bay Area call center to provide additional phone power, enabling the city to reach hundreds of residents at a time, according to Sheryl Contois, police communications coordinator. In addition, the city will create its own phone directory, foregoing the one used by the police dispatch center−−which doesn't contain cell−phone numbers but does include businesses with hundreds of phone lines. The city's new database will allow each household to specify two phone numbers to be called: one during the day, and another in the evening, Contois said. That will cut down on having to call multiple phone lines per residence or business.
Source: http://www.paloaltoonline.com/news/show_story.php?id=1214

[Return to top]

## Information Technology and Telecommunications Sector

28. *April 06, USA TODAY* — **Internet speeds could soon be up to 1,600% faster.** The cable industry's standard−settings unit, CableLabs, plans to endorse this month technology that will let operators boost speeds 400% to 1,600%, over their existing lines. Motorola and Cisco are among the companies offering alternative methods to increase broadband speeds by linking together the bandwidth used for four or more conventional TV channels. While cable operators now usually transmit broadband at three million bits per second (3MB), a download of "a billion bits per second is completely doable," Comcast CEO Brian Roberts said at the National Cable & Telecommunications Association's (NCTA) annual convention in San Francisco this week. This could dramatically affect how people use the Internet when the new modems to handle the speeds arrive, which is expected to be in 2008. These speeds could allow quick sending of detailed images, such as X−rays. "You'll do the majority of your health care straight from the home," says Cisco Systems CEO John Chambers. Hospitals and schools also may be among the first to take advantage of the additional transmission capacity. The new cable standard, known as DOCSIS 3.0, also will make it easier for operators to handle other chores.
NCTA Website: http://www.ncta.com/
Source: http://www.usatoday.com/tech/news/2005−04−05−speed−usat_x.ht m

29. *April 05, Secunia* — **BakBone NetVault buffer overflow vulnerabilities.** Some vulnerabilities in BakBone NetVault, which can be exploited by malicious people to compromise a vulnerable system. The vulnerabilities are caused due to some boundary errors in the communication handling. This can be exploited to cause a heap−based buffer overflow by sending some specially crafted traffic to port 20031. There is no vendor solution at this time.
Source: http://secunia.com/advisories/14814/

30. *April 05, Associated Press* — **New York lawmakers target modem hijacking.** New York state lawmakers unveiled a bill Monday, April 4, that is believed to be the first in the nation to target modem hijacking, a practice in which thieves tap into people's computer modems to

make international phone calls. If passed, the law would allow telephone companies and the state attorney general to bring lawsuits against modem hijackers and their accomplices. The hijackers tap into people's modems by luring computer users to specific Websites – sometimes through e−mails – where pop−up windows emerge inviting the user to click on them. The windows authorize the downloading of modem software that is then remotely accessed to make international calls that are charged back to the user. Consumers can fight hijacking by using a dedicated phone line for the computer dial−up connection, then blocking international calls to that line.
New York Legislature: http://www.state.ny.us
Source: http://www.nytimes.com/aponline/technology/AP−Modem−Hijackin g.html

31. *April 05, CNET News* — **Instant messaging threats rising sharply, reports confirm.**
According to a report issued Tuesday, April 5, by the IMlogic Threat Center – an industry consortium led by security software maker IMlogic – the quantity of instant messaging (IM) threats increased 250 percent in the first quarter of 2005, compared with the same period last year. The research, which tracks viruses, worms, spam and phishing attacks sent over public IM networks, also contends that reported incidents of newly discovered IM threats have grown by 271 percent this year. In addition, the study found that more than 50 percent of the incidents reported to the Threat Center during the first quarter of 2005 involved attacks at workplaces where freely available IM software such as AOL Instant Messenger, MSN Messenger, Windows Messenger, and Yahoo Messenger is used. Based on that data, the consortium advises that companies take a closer look at managing IM security issues.
Report: http://imlogic.com/news/press_107.asp
Source: http://news.com.com/IM+threats+rise+sharply%2C+report+confir ms/2100−7349_3−5655267.html

## Internet Alert Dashboard

### DHS/US−CERT Watch Synopsis

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

**US−CERT Operations Center Synopsis:** US−CERT 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** | 6346 (gnutella−svc), 445 (microsoft−ds), 135 (epmap), 20525 (−−−), 1433 (ms−sql−s), 139 (netbios−ssn), 80 (www), 1026 (−−−), 1027 (icq), 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

**32.** *April 06, Green Bay Press−Gazette (WI)* — **Separate bomb threats close downtown library, evacuate Wal−Mart.** A bomb threat closed the Central Brown County Library for about an hour Tuesday, April 5, after a handwritten note was found in a bathroom. Library staff contacted Green Bay police, then opted to search the building themselves for anything suspicious. As a safety precaution, the Encompass Child Care sent children home with parents or transferred them to another Encompass site, said executive director Rose Smits. Meanwhile, a bomb threat was phoned into Wal−Mart, in Bellevue. Customers were evacuated and Brown County Sheriff Department officials along with K−9 dogs searched the store, but nothing was found, Lt. Steve Perry said.
Source: http://www.greenbaypressgazette.com/news/archive/local_20508 242.shtml

**33.** *April 06, The Times Leader (OH)* — **Part of hospital evacuated for bomb threat.** What turned out to be just an empty piece of plastic pipe had emergency officials taking a bomb threat very seriously Tuesday, April 5, at Trinity Medical Center West in Steubenville, OH. According to Steubenville Police Chief William McCafferty, an employee at Trinity West received a telephone voice mail message early Tuesday concerning a bomb left in the building. At about 9:30 a.m., hospital officials found an approximately 18−inch PVC pipe with duct tape on its ends in a planter. The hospital initiated its emergency protocol and immediately called 911. "It looks real enough," McCafferty said. Steubenville Fire Chief Terri Kovach said the pipe was found in a planter in a common stairwell on the seventh floor of the hospital. About 40 employees in nearby offices on the sixth, seventh and eighth floors were evacuated. Officials from the Steubenville police and fire departments, as well as the Jefferson County Sheriff's Department, spent most of the day on scene waiting for the Youngstown Police Department Bomb Squad to arrive and remove the device. Bomb experts from Youngstown removed the suspected bomb about 1:30 p.m. using a remote−controlled robot.
Source: http://www.timesleaderonline.com/news/story/046202005_new02_ hosptal6.asp

**34.** *April 06, Washington Post* — **Fireproofing blown off Twin Towers.** The hijacked airplanes that struck the World Trade Center on September 11, 2001, hit with such force that the resulting explosions blew the fireproofing off the steel columns, accelerating heat buildup and weakening the structural core −− contributing to the towers' eventual collapse, according to a study issued Tuesday, April 5, by the National Institute of Standards and Technology. The study concluded that no amount of fireproofing could have saved the building. The report found that building codes lacked requirements sufficient to protect the structure of emergency stairwells. Had such codes been in place, said S. Shyam Sunder, the lead investigator of the institute, "there would have been greater opportunity for people to evacuate." The institute's report on the building collapse was long awaited by city officials. The institute based its analysis on extensive interviews with about 1,000 survivors, computer modeling, recovered steel and

communications records. The institute will use the findings in the 3,000−page report to formulate recommendations −− expected for release in September −− for changes in national building codes for office towers. A spokesperson at the Port Authority of New York & New Jersey, which owned the World Trade Center, said local and state officials will review the recommendations and use them to guide reconstruction at Ground Zero.
Investigation findings: http://www.nist.gov/public_affairs/releases/wtc_briefing_apr il0505.htm
Source: http://www.washingtonpost.com/wp−dyn/articles/A28318−2005Apr 5.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.