Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 27 May 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

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

Daily Highlights

- U.S. News reports a computer containing the names and government credit card account numbers for 80,000 Department of Justice personnel is missing from the headquarters of Omega World Travel, which handles business travel arrangements for the department. (See item 7)
- The Washington Post reports that private flights carrying politicians, business executives, and others will be allowed to return to Reagan National Airport by the end of the summer under a plan announced by federal officials that enacts the strictest safety requirements in the country. (See item 11)
- The Hickory Daily Record reports some North Carolina firefighters are using a new program called E−Plan: a government Website designed to inform first responders about hazardous materias. (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. *May 26, Associated Press* — **Some nuclear plants lack backup power for sirens according to commission.** A power failure would disable the community warning sirens at 28 nuclear power plants around the country, the Nuclear Regulatory Commission (NRC) said. The plants

lack backup electricity for the sirens that warn of reactor emergencies and other problems, the NRC said. Seventeen plants have full backup for the systems, while another 18 have at least some sirens that would remain operable during an outage. The sirens are meant to alert residents in a 10−mile radius of trouble. Working sirens would be crucial during a power failure since a loss of electricity can challenge nuclear plants' safety shutdown systems and heighten the risk of a core−melting accident, the groups said. Siren upgrades are in process at about half the plants that lack warning systems that are fully backed up, the NRC said.
Source: http://www.onnnews.com/Global/story.asp?S=3394275

2. *May 25, Rutland Herald (VT)* — **Nuclear plant's emergency plans undergo biennial testing.** A three−day test of Vermont Yankee's emergency plan began Tuesday, May 24, as officials from three states simulated a drill involving two earthquakes that led to the release of radiation from the Vernon, VT, nuclear power plant. Under the scenario, two earthquakes Tuesday morning damaged fission product barriers at the plant, causing a radiation leak and the evacuation of several towns in the surrounding three states. It was the second test of the plant's emergency plans since the terrorist attacks of September 11, 2001. Officials from the Nuclear Regulatory Commission and Federal Emergency Management Agency observed all aspects of the drill Tuesday, from plant employees shutting down the reactor in a mock control room to company and state officials briefing local and national media. On Wednesday, May 25, and Thursday, May 27, emergency management agencies from the Vermont, New Hampshire, Massachusetts and New York will continue tracking the path of the imaginary radioactive plume, according to Michael Slobodien, director of emergency programs for Entergy Nuclear, the plant's owner. The general test of the plant's emergency plans is conducted every two years; the test of the radioactive plume ingestion path is conducted every six years.
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20050525/NEWS/505250376/0/FRONTPAGE

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *May 26, The Reporter (CA)* — **Sulfuric acid spill at California factory keeps area workers and students inside.** A 300−gallon spill of sulfuric acid at a Fairfield, CA factory sent three people to the hospital with burning eyes Wednesday, May 25, and kept hundreds of others inside workplaces and schools while officials neutralized the chemical. Firefighters received a report of the spill at the Rexam Beverage Can Americas Company about 8:30 a.m. (PDT), said Brian Hampton, assistant fire marshal with the Fairfield Fire Department. All Rexam employees evacuated the building; two drove to the hospital with burning eyes. One firefighter was sent to the hospital with the same complaint, Hampton said. Firefighters advised nearby businesses to close all their windows and doors and to keep employees inside until hazardous materials personnel could neutralize the acid with lime, Hampton said. Area elementary and high school students and staff also were told to stay indoors until mid−afternoon. The Napa County hazardous materials team spent approximately eight hours neutralizing the acid.
Source: http://www.thereporter.com/news/ci_2762191

[Return to top]

Defense Industrial Base Sector

4. *May 26, CNET News.com* — **Witty worm may have been targeting a U.S. military base.** A year after the Witty worm infected over 12,000 servers worldwide in just 75 minutes, researchers say they have discovered where the worm started and that the attack might have been an inside job. Witty hit the Internet on March 19, 2004, taking advantage of a flaw in products from Internet Security Systems (ISS). Its payload was malicious, corrupting the information on a system's hard drive. New information on Witty has been compiled by researchers Vern Paxson and Nicholas Weaver, both of the International Computer Science Institute, and by Abhishek Kumar, a student at the Georgia Institute of Technology. The researcher found that the worm was most likely launched from a server at a European Internet service provider and that it was set up to target systems at a U.S. military base. The researchers suspect that Witty was created by an ISS insider. The worm's rapid sprawl was helped by a hit list of 110 vulnerable systems that were infected within 10 seconds of its onset, according to the report. All of the systems were at a single U.S. military installation, the researchers found. "We might then speculate that the attacker knew about the ISS installation at the site," the researchers wrote.
   Research report: http://www.cc.gatech.edu/%7Eakumar/witty−draft.pdf
   Source: http://news.com.com/Witty+worm+traced+to+Europe/2100−7349_3−5721261.html?tag=nefd.top

[Return to top]

Banking and Finance Sector

5. *May 26, Deseret Morning News (UT)* — **Online activities recorded at university.** Investigators seized a computer from a Provo, UT, residence Wednesday, May 25, and said they have identified a man they believe secretly recorded the online activities of Brigham Young University (BYU) students who used four campus computers last month. The computer seized Wednesday does not belong to the man, who hasn't been contacted by police, campus police Lt. Arnie Lemmon said. Investigators would not say if the man was a BYU student, though one administrator previously said he suspected an inside job. The investigation began April 21 when a student attendant noticed a strange icon on the screen of a computer in an open−access computer lab. A search found the icon deeply hidden inside three additional machines and also uncovered its meaning −− someone had loaded keystroke logger software on the four computers. The sophisticated program recorded the keystrokes of more than 600 students and periodically sent the information to a Hotmail e−mail account. The keystroke logger captured student passwords and other personal information, but none of the students has reported any identity theft or other unusual account activity to BYU administrators or police.
   Source: http://deseretnews.com/dn/view/0,1249,600136721,00.html

6. *May 26, Westchester.com* — **International counterfeit check ring caught in New York.** New York District Attorney Jeanine Pirro was joined on Wednesday, May 25, by Raymond Martinez, Commissioner of New York State Department of Motor Vehicles, to announce the arrests of nineteen members of an international check counterfeiting ring. The arrests were the result of a joint investigation that included various law enforcement organizations in the New

York area. Late last week, members of a counterfeit check ring entered Westchester County, NY, and began operating out of three motel rooms in Elmsford, with the intent to flood the region with counterfeit checks. Investigators watched them, and when they tried to exchange the fake checks for cash, all nineteen individuals were arrested. The Westchester County District Attorney's Office is working with Federal authorities to determine the extent of any ties between these defendants and some ruthless street gangs, including Florencia 13 and Aztec Nation who have recently been reported as having moved aggressively into the counterfeit document business, branding it with violence and intimidation.
Source: http://westchester.com/Westchester_News/Westchester_Government_and_Politics/International_Counterfeit_Check_Ring_Caught_In_Westchester_200505265278.html

7. *May 25, U.S. News* — **Government credit cards at risk after computer is lost.** The government agency that prosecutes identity thefts now finds itself in the role of potential victim. A computer containing the names and government credit card account numbers for 80,000 Department of Justice personnel is missing from the Fairfax, VA, headquarters of Omega World Travel, which handles business travel arrangements for the department. Department of Justice spokesperson Gina Talamona said that the computer disappeared sometime between May 7 and May 9. It contained password−protected names, travel card account numbers, prior lost/stolen card accounts, and expiration dates for the credit cards, but no personal address information, Social Security numbers, or employees' office locations. A May 13 memo issued to Justice executives states that JPMorgan, Chase, and Bank One, the issuers of the credit cards, are monitoring the Department of Justice accounts for suspicious activity, but so far, nothing has attracted suspicion.
Source: http://www.usnews.com/usnews/news/articles/050525/25webid.ht m

8. *May 25, The Stanford Daily (CA)* — **Students' files hacked at career center.** The Career Development Center (CDC) at Stanford University in Stanford, CA, notified students Tuesday, May 24, that its computer system was "improperly accessed from outside of the Stanford network" on May 11. Information available on the Website was limited to files that generally include names, resumes, letters of recommendation and Social Security numbers. It is still unknown who hacked into the site, which included information from 1996 to the present. No student financial, credit card, driver's license or government identification information was available at the time of the intrusion. However, recruiter files contained credit card numbers. In response to the intrusion, Stanford temporarily disabled the CDC's system and reported the incident to the Federal Bureau of Investigation. The San Jose field office is looking into the incident.
Source: http://daily.stanford.edu/tempo?page=content&id=17516&reposi tory=0001_article

[Return to top]

Transportation and Border Security Sector

9. *May 26, Government Accountability Office* — **GAO−05−466T: Homeland Security: Key Cargo Security Programs Can Be Improved (Testimony).** U.S. Customs and Border Protection (CBP) has in place two programs to help address the threat posed by terrorists smuggling weapons of mass destruction (WMD) into the United States: the Customs−Trade

Partnership Against Terrorism (C−TPAT) and the Container Security Initiative (CSI). In July 2003, the Government Accountability Office (GAO) reported that these programs had management challenges that limited their effectiveness. Given plans to expand both programs, in two recently issued reports GAO examined selected aspects of both programs' operations. This statement is a summary of those publicly available reports. For the C−TPAT program, GAO recommended that CBP eliminate the weaknesses in its validation process, complete its human capital plan and performance measures, and put in place internal controls for the program. For the CSI program, GAO recommended that CBP refine its staffing model to help improve targeting of shipments at CSI ports, develop minimum technical requirements for the capabilities of inspection equipment, and complete development of program measures. CBP generally concurred with the recommendations and described corrective actions to respond to them.
Highlights: http://www.gao.gov/highlights/d05466thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−466T

10. *May 26, Government Accountability Office* — **GAO−05−755T: National Airspace System: Initiatives to Reduce Flight Delays and Enhance Capacity are Ongoing but Challenges Remain (Testimony).** Since the unprecedented flight delays in 2000, a year in which one in four flights were delayed, the U.S. aviation system has been adversely affected by many unanticipated events −−such as the September 11th terrorist attacks, and Severe Acute Respiratory Syndrome (SARS) −− that significantly reduced the demand for air travel. However, demand for air travel is rebounding. For example, the number of passengers traveling by air increased from 642 million in 2003 to 688 million in 2004. Flight delays have been among the most vexing problems in the national transportation system and are defined by the Department of Transportation as instances when aircraft arrive at the gate 15 minutes or more after scheduled arrival time. In 2004, one in five flights were delayed primarily at New York La Guardia and Chicago O'Hare. Delays at these airports have consequences for the rest of the system. The Government Accountability Office's testimony addresses the following questions that pertain to flight delays and enhancing capacity: (1) What initiatives are ongoing by the federal government, airlines, and airports to address flight delays and enhance capacity? (2) What are some of the challenges in reducing flight delays and enhancing capacity? (3) What other options are available for reducing flight delays and enhancing capacity?
Highlights: http://www.gao.gov/highlights/d05755thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−755T

11. *May 26, Washington Post* — **Private flights to resume at National under strict limits.** Private flights carrying politicians, business executives and others will be allowed to return to Reagan National Airport by the end of the summer under a plan announced on Wednesday, May 25, by federal officials that enacts the strictest safety requirements in the country. Citing national security, the federal government had banned the small planes from the airport −− which is just across the Potomac River from downtown Washington −− since the September 11, 2001, terrorist attacks. To access National under the new rules, crews and passengers will undergo background checks, all bags will be screened, armed security guards paid for by the fliers must be on board, flights can come from only 12 designated airports, and passenger and crew lists must be submitted 24 hours in advance. Federal officials said 48 flights would be allowed per day, fewer than half the approximately 100 general aviation flights that shuttled in and out of National each day before the terrorist attacks.

Department of Homeland Security rules for National flights:
http://www.dhs.gov/dhspublic/display?content=4518
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/05/25/AR2005052500264.html?sub=AR

12. *May 26, American Trucking Associations* — **Trucking industry has shortage of drivers.** The long−haul, heavy−duty truck transportation industry in the United States is experiencing a national shortage of 20,000 truck drivers, the American Trucking Associations (ATA) reported on Wednesday, May 25, in its newly released U.S. Truck Driver Shortage: Analysis and Forecasts report. The Forecast, a report on the present and future of the long−haul truck driver pool, predicts the shortage of long−haul truck drivers will increase to 111,000 by 2014 if current demographic trends stay their course and if the overall labor force continues to grow at a slower pace. “The driver market is the tightest it has been in 20 years,” ATA President and CEO Bill Graves said. “It’s a major limitation to the amount of freight that motor carriers can haul. It’s critical that we find ways to tap a new labor pool, increase wages and recruit new people into the industry that keeps our national economy moving.” Of the 3.4 million truck drivers on the road, 1.3 million are long−haul truckers, the driver segment most severely impacted by the shortage. The driver shortage comes as the trucking industry is hauling more freight than ever. Total annual tonnage hauled by truck is expected to increase to 13 billion tons by 2016 from 9.8 billion tons in 2004.
Forecast report: http://www.truckline.com/NR/rdonlyres/EFEEB145−58B7−4C1A−AE19−33BED578D7AF/0/ATADriverShortageStudy05.pdf
Source: http://www.truckline.com/NR/exeres/C36957C4−EF4B−4DB4−9A6C−B597A3DFB8AC.htm

13. *May 26, Associated Press* — **Secretary Mineta calls on Amtrak to cut costs.** Department of Transportation Secretary Norman Y. Mineta is urging Amtrak to immediately put in place cost−cutting measures, saying the railroad could be as much as $40 million in debt before September 30. In a letter sent late Wednesday, May 25, to Amtrak President David Gunn, Mineta said Amtrak should cut costs by "reducing expenses and conserving cash in a manner that does not jeopardize safety." Mineta did not state how much money Amtrak should be trying to cut. Mineta also wrote that Amtrak cannot continue to spend at current levels because the brake problems with the Acela Express trains is costing the railroad about $1.25 million per week in revenues. Acela's entire 20−train fleet was taken out of service in April after cracks were found in some of the trains’ disc brake rotors. The cause of the problem is still not known.
Text of the letter: http://www.dot.gov/affairs/dot8305.htm
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−amtrak,0,3057730.story?coll=sns−ap−nation−headlines

14. *May 26, Associated Press* — **Border patrol cuts back at checkpoint.** The U.S. Border Patrol has dramatically curtailed operations at a traffic checkpoint along Interstate 91 at the Hartford, VT, rest area, 97 miles from the Canadian border. Assistant Chief Patrol Agent John Pfeifer of the Border Patrol's Swanton Sector said the cuts were not in response to criticisms about government intrusions nearly 100 miles from the border, but were due to more staff being needed elsewhere, particularly the Southwest. The Swanton sector covers the three northernmost counties in New Hampshire, all of Vermont, and upstate New York to Ogdensburg. Other interior checkpoints include a stop in North Hudson, NY, along Interstate

87. The Hartford checkpoint began being staffed on a daily basis in December 2003, and as of last month, 640 people had been arrested there on immigration−related matters.
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20050526/NEWS/505260408/1003/NEWS02

[Return to top]

Postal and Shipping Sector

15. *May 25, News Sun (IL)* — **Postal Service emergency exercise held.** The emergency preparedness exercise held Tuesday, May 24, at the U.S. Postal Service Carol Stream, IL, Processing & Distribution Center is a precursor to a similar exercise to be held later this year at the Palatine center which handles Lake County mail, a postal official said. The exercise at the Fullerton Avenue facility included an evacuation and biohazard detection system response. The Carol Stream Post Office was closed from 4 to 4:45 p.m. during the exercise. The exercise tested preparedness plans to protect employees in the event of a biohazard detection system alert, said Tim Ratliff, Postal Service spokesperson. "The Postal Service has partnered with local first−responders and public health officials to develop plans to protect employees and the response exercise provides an opportunity to test emergency preparedness plans," Ratliff said. Participating in Carol Stream were police departments from Carol Stream and Glendale Heights, Carol Stream Fire Protection District, U.S. Postal Inspection Service, Illinois Department of Public Health, DuPage County Health Department, Illinois Emergency Management Agency, Office of Homeland Security and Emergency Management, American Red Cross of Greater Chicago, the FBI and Suburban PACE bus company.
Source: http://www.suburbanchicagonews.com/newssun/city/w25postal.ht m

[Return to top]

Agriculture Sector

16. *May 26, Orlando Sentinel (FL)* — **Chippers may fuel citrus canker.** Some experts say −− and some of Florida's research shows −− that chipping sends clouds of canker bacteria−laden debris into the air, where it can be carried in the wind before drifting onto other plants. State officials say there's little chance of that causing new infections, but others suggest it is a legitimate concern. In the 1990s, a leading citrus−canker researcher with the federal government warned it could spread the disease. The state briefly stopped. Instead, crews took whole trees or large parts of them and put them in a compactor before taking them to a landfill. Overwhelmed by the volume of trees it was destroying, the state soon returned to chipping. Compacting "was just impractical," said Tim Schubert, a plant pathologist with the Florida Department of Agriculture. The Florida Agriculture Department destroys all citrus trees −− healthy or not −− within 1,900 feet of an infected tree. Canker causes blemishes on fruit, reduces citrus production, and triggers international shipping bans. In commercial groves, workers typically bulldoze condemned trees into piles before setting them on fire. But in residential areas, crews chip them, a process the state acknowledged isn't ideal.
Source: http://www.orlandosentinel.com/news/orl−locvcanker26052605may26,0,6351166.story?coll=orl−news−headlines

17. *May 26, Casper Star Tribune (WY)* — **New brucellosis agreement proposed.** Cattlemen and conservationists gave differing opinions Wednesday, May 26, on a yet−to−be−signed agreement among state and federal agencies to eradicate brucellosis in the greater Yellowstone ecosystem. Conservationists say they worry the proposal signals a shift toward more aggressive tactics to combat the disease that would treat wildlife like livestock. Cattlemen say a more aggressive approach is long overdue. At a meeting of the Greater Yellowstone Interagency Brucellosis Committee, a new "memorandum of understanding" to guide the group was proposed that includes language shifts from the current agreement. Instead of the current language calling for the development of plans to eradicate the disease, the new language calls simply for its elimination. Rob Hendry of the Wyoming Stock Growers Association said the committee has been "talking about getting rid of brucellosis in Yellowstone" for the last 10 years. "I haven't seen much progress," he said, and that is "unacceptable." Wyoming has lost its brucellosis−free status in cattle because of herds being infected with the disease, likely from wildlife. The memorandum −− crafted by federal agencies and presented to the group by U.S. Department of Agriculture Undersecretary Bill Hawks and Paul Hoffman, deputy assistant undersecretary of the Department of Interior −− has yet to be signed by the governors of Wyoming, Montana, and Idaho.
Source: http://www.casperstartribune.net/articles/2005/05/26/news/wyoming/25b45fb91d9be9d28725700c0083bd4f.txt

[Return to top]

Food Sector

18. *May 26, Food Ingredients First* — **Cargill completes Citrico acquisition.** Cargill has completed the acquisition of the global pectin business of Citrico, a manufacturer and international supplier of citrus products for the food, beverage, and pharmaceutical industries. Citrico’s pectin production and sales operations in Malchin, Germany, will become part of Cargill’s texturizing business in Germany. Cargill announced plans for the acquisition of Citrico in March 2005. The $58.5 million valued manufacturer and international supplier of citrus products went into liquidation in December 2004.
Source: http://www.foodingredientsfirst.com/newsmaker_article.asp?idNewsMaker=8274&fSite=AO545&next=1

19. *May 25, Food and Drug Administration* — **Ground basil recalled.** American Natural Herbs & Spices Inc., of Union City, CA, is recalling the following product because it may be contaminated with Salmonella: " aSPICES Brand BASIL GROUND" Salmonella is an organism which can cause serious and sometimes fatal infections in young children, frail, or elderly people and others with weakened immune systems. Most cases resolve without the need for medical attention. However, some persons infected with salmonella may experience fever, diarrhea, nausea, vomiting, and abdominal pain. No illnesses have been reported to date in connection with this product. The contamination was identified when routine testing conducted by the California Department of Health Services revealed the presence of salmonella in a sample of "aSPICES brand Basil ground." The recalled aSPICES Brand product was sold in supermarkets throughout California.
Source: http://www.fda.gov/oc/po/firmrecalls/american05_05.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

20. *May 26, Agence France Presse* — **China claims it has new vaccines to fight bird flu.** Chinese scientists have developed two new vaccines which they claim are fully capable of stopping the spread of the deadly H5N1 strain of bird flu in birds and poultry. The announcement came as U.S. scientist David Ho warned China remained woefully ill equipped for tackling avian flu. Chen Hualan, director of the China National Bird Flu Reference Laboratory, said the new vaccines had proved to be a success. They passed a state−level appraisal and received permission from China's Ministry of Agriculture to be sold on the market. However, the World Health Organization (WHO) cautioned that while some bird flu vaccines were effective by reducing the amount of virus in the birds, others may be masking the problem. "In some cases, there's an argument that what you're reducing are the symptoms in birds, but that they still have the virus and are still shedding the virus," Maria Cheng, a Beijing−based WHO spokesperson said. The vaccine news came as China was gripped by the first confirmed outbreak of bird flu in nearly a year after migratory birds were found to have died from H5N1 in northwest Qinghai province. The discovery launched the country into a massive vaccination drive which aims to cover three million birds.
Source: http://news.yahoo.com/s/afp/20050526/hl_afp/healthchinafluva ccine_050526110524

21. *May 26, Associated Press* — **World health groups commit to immunization plan.** Member states adopted a 10−year global strategy to immunize more people from more diseases as the World Health Organization (WHO) wrapped up its annual meeting Wednesday, May 25. Delegates to the World Health Assembly committed to a joint WHO and UNICEF plan to have each country have 90 percent of its population immunized by 2010 and prevent up to five million child deaths a year by 2015. Vaccine−preventable diseases kill more than two million people each year, two−thirds of whom are young children. The campaign aims to reach more people in isolated areas and will target a broader age group to include adolescents and adults as well as children and the elderly. The plan is to introduce a range of new vaccines against killers such as rotavirus, which causes acute diarrhea; pneumococcal disease, which leads to pneumonia; meningitis A; cervical cancer; and Japanese encephalitis.
Source: http://www.orlandosentinel.com/features/health/orl−asecwho26 052605may26,0,5752352.story?coll=orl−home−headlines

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

22. *May 26, Hickory Daily Record (NC)* — **North Carolina emergency workers to use Hazmat program.** Catawba County first responders are the first in North Carolina to use a Website that gives information about hazardous chemicals in case of a fire or spill. Hickory firefighters are training on the new program, called E−Plan. The department bought 12 laptop computers to install in the fire engines. The computers were purchased with money from an $85,000 grant and about $8,000 from the city. The laptops are fireproof. That means the computers are strong enough to be dropped six feet on concrete and not be damaged. The computers also are programmed to recognize and open by the fingertip of the firefighters. The laptops are capable of receiving Internet connections anywhere because of a satellite wireless card. Once installed, the laptops will be used to access E−Plan on the way to a call. E−Plan is a Website operated by the U.S. Environmental Protection Agency. It is designed to inform first responders about hazardous materials found at certain companies or on tanker trucks. The program also can help with evacuation routes, emergency contacts, first aid and chemical profiles.
Source: http://www.hickoryrecord.com/servlet/Satellite?pagename=HDR/MGArticle/HDR_BasicArticle&c=MGArticle&cid=1031782936384&pat h=!news!localnews

23. *May 23, Northjersey.com* — **Aid crews respond to simulated attack on train.** There was no smoke, no sirens, and no blood. But that didn't make the Sunday, May 22, simulated terrorist attack explosion at the Ramsey, NJ, Route 17 train station and the ensuing rescue efforts any less important to the 200 or so participating police officers, firefighters, and rescue squad members. More than a year in the planning, Operation Safe Platform was one town's way to prepare for the kind of terrorist attack it never thought about before 9/11. So for two hours Sunday, emergency crews from Ramsey and neighboring towns, along with units from state, county and transit agencies, took part in a full−scale exercise plan designed to provide participants with an overview of their roles and responsibilities in a terrorist incident. The drill was built around a simulated explosion on an NJ Transit commuter train. The responders had general knowledge of what was coming, but details were confidential until Sunday. As a result, emergency personnel had to respond to events as they unfolded. "We wanted to make it as |real to life as possible," said Sgt. Angelo LaManna, a Ramsey policeman and a deputy coordinator of the borough's Office of Emergency Management.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjcxN2Y3dnFlZUVFeXkyJmZnYmVsN2Y3dnFlZUVFeXk2Njk3Ndkx

[Return to top]

Information Technology and Telecommunications Sector

24. *May 27, Associated Press* — **Federal agents shut Website in piracy crackdown.** The government announced a crackdown Wednesday, May 25 on the theft of movies and other copyright materials. Federal agents shut down a Website that they said allowed people to download the new “Star Wars” movie even before it was shown in theaters. The Elite Torrents site was engaging in high−tech piracy by letting people download copies of movies and other

copyright material for free, authorities said. The action was the first criminal enforcement against individuals who are using cutting−edge BitTorrent software to obtain pirated content online, Department of Justice and Department of Homeland Security officials said. Elite Torrents had more than 133,000 members and offered 17,800 movies and software programs in the past four months, officials said. “Today's crackdown sends a clear and unmistakable message to anyone involved in the online theft of copyrighted works that they cannot hide behind new technology,” said John C. Richter, acting assistant attorney general. BitTorrent has become the file−sharing software of choice because of its speed and effectiveness, especially after the recording industry last year began cracking down on users of Kazaa, Morpheus, Grokster and other established software.
Source: http://www.nytimes.com/aponline/technology/AP−Movie−Download ing.html

25. *May 26, Government Accountability Office* — **GAO−05−434: Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities (Report).** As the focal point for critical infrastructure protection (CIP), the Department of Homeland Security (DHS) has many cybersecurity−related roles and responsibilities. DHS established the National Cyber Security Division to take the lead in addressing the cybersecurity of critical infrastructures. While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the responsibilities. DHS faces a number of challenges that have impeded its ability to fulfill its cyber CIP responsibilities. These key challenges include achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, achieving two−way information sharing with these stakeholders, and demonstrating the value DHS can provide. In its strategic plan for cybersecurity, DHS identifies steps that can begin to address the challenges. However, until it confronts and resolves these underlying challenges and implements its plans, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our critical infrastructures. In written comments on a draft of this report, DHS agreed with the Government Accountability Office’s recommendation to engage stakeholders to prioritize its responsibilities, but disagreed with and sought clarification on recommendations to resolve its challenges.
Highlights: http://www.gao.gov/highlights/d05434high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−434

26. *May 25, FrSIRT* — **GNU Mailutils multiple remote code execution vulnerabilities.** Multiple vulnerabilities were identified in GNU Mailutils, which may be exploited by remote or local attackers to execute arbitrary commands or cause a denial of service. These issues are due to format string, input validation, integer overflow, and buffer overflow errors.
Upgrade to GNU Mailutils version 0.6.90: ftp://alpha.gnu.org/gnu/mailutils/
Source: http://www.frsirt.com/english/advisories/2005/0623

27. *May 25, SecurityFocus* — **SCO OpenServer NWPrint command line argument local buffer overflow vulnerability.** NWPRINT that is distributed with SCO OpenServer is prone to a local buffer overflow vulnerability. This issue arises because the application fails to perform boundary checks prior to copying user supplied data into sensitive process buffers. A local attacker can gain elevated privileges by exploiting this issue.
Updates available: http://www.securityfocus.com/advisories/8622

Source: http://www.securityfocus.com/bid/12986/info/

28. *May 25, SecurityFocus* — **PHP Poll Creator poll PHP remote file include vulnerability.** PHP Poll Creator is affected by a remote file include vulnerability. This issue is due to a failure in the application to properly sanitize user supplied input. This flaw is due to a "PHP File Inclusion" identified in the "poll_vote.php" script that does not properly filter the "relativer_pfad" variable, which may be exploited by an attacker to include an arbitrary file and execute remote commands with the privileges of the web server. There is no solution at this time.
Source: http://www.securityfocus.com/bid/13760/info/

29. *May 25, SecurityFocus* — **Ethereal multiple remote protocol dissector vulnerabilities.** Many vulnerabilities in Ethereal have been disclosed by the vendor. The reported issues are in various protocol dissectors. These issues could allow remote attackers to execute arbitrary machine code in the context of the vulnerable application. Attackers could also crash the affected application.
Vendor updates available: http://www.securityfocus.com/bid/13504/solution/
Source: http://www.securityfocus.com/bid/13504/discussion/

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 a remote exploitation of a format string vulnerability in the imap4d server within version 0.6 of the GNU Project's Mailutils package could allow an unauthenticated attacker to execute arbitrary code. The imap4d server allows remote users to retrieve their email via the Internet Message Access Protocol, Version 4rev1 as specified in RFC3501. This is a client/server protocol supported by a large number of email clients on multiple platforms.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 2745 (Bagle.C), 1026 (−−−), 139 (netbios−ssn), 5000 (BackDoorSetup), 5554 (sasser−ftp), 65506 (phatbot−ssl), 9898 (dabber), 1434 (ms−sql−m) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

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 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) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 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