Department of Homeland Security Daily Open Source Infrastructure Report for 26 May 2006

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

Daily Highlights

- Computerworld reports the American Red Cross has warned about one million blood donors in the Missouri−Illinois Blood Services Region that personal information about them could have been stolen earlier this year by a former employee and might have been used in identity thefts. (See item 14)
- The Associated Press reports power was restored Thursday, May 25, throughout the heavily traveled New York to Washington rail corridor, after a power outage stranded thousands of rush−hour commuters, stopping trains inside tunnels and forcing many passengers to get out and walk. (See item 19)

DHS Daily Open Source Infrastructure Report *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://www.esisac.com]

1. *May 24, Patriot−Ledger (MA)* — **Uranium missing at power plant: Officials say tiny rods probably not stolen; likely the result of a bookkeeping error.** A tiny amount of highly radioactive uranium is missing from the Pilgrim nuclear power plant, prompting workers there to notify the Nuclear Regulatory Commission and launch an investigation. Two monitoring rods each about the size of a ball point pen and containing .003 grams of uranium were discovered missing Monday, May 22, from their storage tubes in the plant's spent−fuel pool,

according to Entergy spokesperson David Tarantino. Workers at the plant made the discovery while cleaning out the storage pool in order to ship out low−level waste. The uranium would be of no use to terrorists, but it is enough to produce about 10 millirems of radiation per hour, Tarantino said. Tarantino said it was possible the missing monitors were doubled up in other tubes or have already been shipped out of the plant. "It could be a bookkeeping or inventory error," Tarantino said. "It's unlikely they could have left the plant except in a low level shipment because they would have set off the alarms," Tarantino said.
Source: http://ledger.southofboston.com/articles/2006/05/24/news/new s07.txt

2. *May 24, Reuters* — **FERC: U.S. needs both Alaska pipeline, LNG terminals.** U.S. demand for natural gas will be strong enough in the future to support both a planned pipeline to bring Alaskan gas to the lower 48 states and the many liquefied natural gas (LNG) import terminals that will be built, Federal Energy Regulatory Commission (FERC) head Nora Brownell said on Wednesday, May 24. FERC has approved several LNG imports terminals and dozens more have been proposed. At the same time, a coalition of large energy companies is trying to work out the terms for building a huge natural gas pipeline in Alaska to supply the U.S. mainland. The U.S. market will be able to absorb the expected boost in available gas from the two supply streams, according to Brownell. "There's room for both" because U.S. gas demand will also increase and prices will be high enough to make the projects profitable, Brownell said at the Reuters Global Energy Summit in New York. However, she said "there's just no way" all the proposed LNG terminals will be built, not due to competition from the Alaskan pipeline, but because there will not be enough LNG imported to support them.
Source: http://news.yahoo.com/s/nm/20060524/us_nm/energy_summit_natg as_supplies_dc_1

3. *May 24, Associated Press* — **Investigators: Burst pipe caused explosion, fire at refinery.** The weekend fire that cut production at the Valero St. Charles refinery in Norco, LA, started when a 12−inch overhead pipe burst in a unit that removes sulfur from crude oil, federal investigators reported Wednesday, May 24. The U.S. Chemical Safety Board team does not know why the pipe broke, a news release from the board said. But board member Gary Visscher said corrosion has caused similar accidents at a number of other refineries. The CSB said the pipe normally carries partly distilled crude as a gas, at about 600 pounds of pressure per square inch. The gas was so hot that it burst into flames when it hit the air. The refinery said it expects gasoline production to return to normal and low sulphur diesel production to about 10,000 barrels a day when other units are restarted at the end of the week.
Source: http://www.nola.com/newsflash/louisiana/index.ssf?/base/busi ness−3/1148508882184170.xml&storylist=louisiana

4. *May 24, Associated Press* — **Fire breaks out in garbage bin at Iowa power plant.** An investigation is under way into a fire in a waste recovery area of a power plant in Ames, IA. On Wednesday, May 24, officials said the fire broke out overnight in a storage bin used to shred garbage, which is then mixed with coal to generate power for the city. Fire Lieutenant Doug Allen says the fire was quickly contained and no one was hurt.
Source: http://www.whotv.com/Global/story.asp?S=4942905&nav=menu100_2

5. *May 24, Orlando Business Journal* — **Kissimmee utility to host hurricane preparation meetings.** The Kissimmee Utility Authority will host a series of neighborhood meetings in June designed to inform the public about disaster preparedness and emergency response. Using

lessons learned from the last two hurricane seasons, the 60−minute sessions will include helpful tips, details on evacuation procedures, power restoration, generator safety, and public safety.
Source: http://orlando.bizjournals.com/orlando/stories/2006/05/22/da ily28.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *May 25, WRAL (NC)* — **North Carolina plant fire prompts delays of inbound flights.** Firefighters battled a massive fire at the Coyne Textile Company late Wednesday evening, May 24, in Charlotte, NC. For a brief time, inbound flights to Charlotte Douglas Airport were delayed because of the threat of explosions within the building.
Source: http://www.wral.com/news/9271153/detail.html

7. *May 25, News 8 Austin (TX)* — **Leaking tanker prompts highway closure, evacuation in Texas.** A 12,000−gallon tanker leaking chlorine fumes shut down all lanes of U.S. Highway 290 at Springdale Road Thursday morning, May 25, said Lt. David Belknap of the Austin, TX, Fire Department. Highway 290, in both directions, was closed as a result. Residents who live north of the intersection were advised to remain indoors and turn off their air conditioners, or evacuate the neighborhood altogether.
Source: http://www.news8austin.com/content/your_news/default.asp?ArI D=162780

[Return to top]

Defense Industrial Base Sector

8. *May 25, Government Accountability Office* — **GAO−06−512: Defense Inventory: Actions Needed to Improve Inventory Retention Management (Report).** Maintaining the right amount and types of items in its inventory −− a key aspect of supply chain management −− has been a long−standing challenge for the Department of Defense (DoD) and has been on the Government Accountability Office's (GAO) list of high−risk areas since 1990. DoD retains inventory above its normal operating requirements for various reasons including for contingency purposes or because it is more economical to keep items than dispose and repurchase them later. DoD’s inventory levels have grown in recent years to almost $80 billion in fiscal year 2005. GAO was asked to assess the management of contingency retention inventory to determine whether (1) the Army, Air Force, Navy, and Defense Logistics Agency have followed inventory guidance and (2) DoD is providing oversight of inventory across these components. Also, GAO provided an update on the progress DoD has made in implementing GAO’s past recommendations on the components’ management of economic retention inventory. GAO recommends that DoD direct the inventory centers to take the steps necessary to follow existing inventory management policies and procedures and provide oversight to ensure the components’ compliance. In reviewing a draft of this report, DoD generally agreed with GAO’s recommendations.
Highlights: http://www.gao.gov/highlights/d06512high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−512

9. *May 22, Government Computer News* — **Intelligence community to reboot security.** The intelligence community is turning to Defense services and agencies, as well as representatives from industry and academia, to help them overhaul their outdated and ineffective certification and accreditation processes. This month, personnel will begin receiving invitations to participate in one of two teams −− a green team and a gold team −− that will ultimately make suggestions on how to improve certification and accreditation processes across the intelligence community. Air Force Maj. Gen. Dale Meyerrose, associate director of national intelligence and CIO of the intelligence community, said he is working with John Grimes, Defense CIO, on the initiative and that the outcome will help the intelligence agencies and components within the services reduce the time needed to certify and accredit standards and systems. He said the teams also would help the intelligence community become more inclusive. “We have to make intelligence fast, agile and transparent,” Meyerrose added. “It doesn’t do us any good to deliver the right information to the right place, but not in the nick of time. But it’s not just about the speed of delivery of intelligence; it’s the speed in which we bring innovation.”
Source: http://www.gcn.com/print/25_13/40824−1.html

[Return to top]

Banking and Finance Sector

10. *May 25, Finextra* — **Barclays fights online fraud with text alerts and free antivirus software.** In a bid to cut online fraud levels, Barclays is providing free virus protection software to customers and is also launching a text messaging service that alerts account holders to new Web transactions. The new SMS alert service will send text messages to notify customers of new payees on their online account. A text message will be sent to customers when an online payment is made to a new payee for the first time, enabling customers to alert the bank immediately if the transaction is suspicious.
Source: http://finextra.com/fullstory.asp?id=15358

11. *May 24, Register (UK)* — **Scammers use stolen credit card data to purchase from spam campaigns.** Scammers who deal in stolen credit card data have devised a means to extract money from sponsors of junk mail campaigns. Carders have signed up as affiliates to spam campaigns, but instead of sending out junk mail themselves they are using stolen credit card data to make purchases from the sponsors of spam campaigns, such as online pharmacies. The carders earn a cut of these sales of anything between 40 to 50 percent, the Washington Post's security blog reports, more than enough to make the scam viable. CipherTrust identified the new ruse during its monitoring of online spam and fraud forums.
Source: http://www.theregister.co.uk/2006/05/24/carders_scam_spammer s/

12. *May 24, Mail & Guardian (South Africa)* — **Bank warns clients about new ATM card scam.** A new variation of card skimming at automated teller machines (ATMs), which gives criminals access to customers' bank accounts, has gripped the country, Absa said on Wednesday, May 24. "Two or three criminals will approach the customer and cancel the transaction. While two criminals keep the customer busy the other criminal takes the customer's card and swipes it through a hand−held skimming device," Venete Klein of Absa said. The thieves, using a hand−held device, make a duplicate copy of the customer's card, giving them full access to the customer's account once he or she has left the ATM. Klein said that in some instances the

criminals also persuade the customer to move to another ATM to process the transaction. "The customer is still able to proceed with the transaction ... but usually the fraud is only discovered when the customer tries to draw money again and there are insufficient funds available." She said criminals usually use the duplicate card by the same afternoon or evening of the robbery.
Source: http://www.mg.co.za/articlepage.aspx?area=/breaking_news/breaking_news__national/&articleid=272651

13. *May 24, CanWest News Service (Canada)* — **Canada fraud scheme linked to terrorist activities.** A criminal cell operating across Canada is funnelling millions of dollars to Dubai to fund terrorist activities through a sophisticated credit/debit card fraud scheme, says Insp. Joan McCallum of Alberta's Integrated Response to Organized Crime unit. It is but one of a number of "extremely prevalent" organized crime groups reaping huge profits from an old crime with a new twist, he says. Improved criminal technology now involves the insertion of a memory chip to record data into keypad terminals customers use at retail counters, gas stations, and restaurants. Criminals target the little black terminals handed to a customer to punch in numbers by simply unplugging them and carrying them off. "A lot of merchants leave those on the counter. The criminal will modify it to add a memory chip to the terminal," said Const. Stephen Macumber of the Calgary police. Because the terminals are generic, and many retail outlets use the same kind, they are easily transferable. When a card is swiped, the data goes to the credit card company. A memory card that's been placed inside records magnetic data for the crime group. "They leave it there a few weeks and go back and steal it again," said Macumber.
Source: http://www.canada.com/cityguides/winnipeg/info/story.html?id=e6515153−8e64−4a98−8c4c−59d35e505d17&k=76134

14. *May 24, Computerworld* — **Red Cross warns blood donors of possible ID thefts in Midwest.** About one million blood donors in the Missouri−Illinois Blood Services Region of the American Red Cross were warned last week that personal information about them could have been stolen earlier this year by a former employee and might have been used in identity thefts. The former worker had access to 8,000 blood donors in a database she used in her job, all of whom were notified of possible identity theft problems on Friday, March 17. After the original warning letters went out, the Red Cross expanded the identity theft warnings to all one million donors in the Missouri−Illinois region because of concerns that she may have accidentally accessed other records in the larger group. At least four of the donors among the original 8,000 in the donor database were victims of the data−theft scheme. The thefts occurred when the former employee, a telephone blood−drive recruiter, entered random numbers of past donors into her 8,000−donor database, then was able to access the names, Social Security numbers, phone numbers, and birth dates of potential victims. The former employee then allegedly opened credit card accounts at several stores using the stolen information and made purchases valued at more than $1,000.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000754

15. *May 24, ABC−6 (PA)* — **Security breach at University of Delaware.** Another hacker attack has occurred at the University of Delaware, where campus officials say the hack on the public safety computer could have exposed names, social security, and drivers license numbers. They believe the hackers were trying to copy database information. The incident happened last month, and letters have been mailed to more than one thousand people whose personal

information may have been stolen.
Source: http://abclocal.go.com/wpvi/story?section=local&id=4203345

16. *May 23, Reuters* — **Hundreds arrested in international fraud schemes.** More than 565 people on three continents have been arrested over the past year as part of an international operation targeting mass−marketing fraud schemes, the U.S. Justice Department said on Tuesday, May 23. The department said about 2.8 million people had fallen victim to the fraud schemes that were carried out through the Internet, by telemarketers and through mass mailings. Losses totaled more than $1 billion. Through "Operation Global Con," police in countries across North and South America and Europe have uncovered a number of scams and have arrested 565 people since March 1, 2005. The majority of the arrests were made in Spain, followed by the U.S, Canada, and the Netherlands. Some of the schemes included sweepstakes fraud, when a victim is told he or she has won a large amount of money in a sweepstakes but must first pay bogus "fees" or "taxes" on the winnings. Other scams include fake offers of "pre−approved" credit cards and loans, offers of nonexistent investments, and tax fraud schemes.
Source: http://today.reuters.com/news/newsArticle.aspx?type=internetNews&storyID=2006−05−23T200556Z_01_N23179986_RTRUKOC_0_US−CRIME−FRAUD.xml&archived=False

[Return to top]

Transportation and Border Security Sector

17. *May 25, Department of Transportation* — **Department of Transportation convenes national commission on surface transportation funding.** Changes in funding, traffic and business trends are posing serious challenges to the nation’s transportation systems that offer a rare opportunity to make a “historic transition” in how existing and new projects are funded, Department of Transportation Secretary Norman Y. Mineta said as he convened the first meeting of the new National Surface Transportation Policy and Revenue Study Commission. Challenges cited by the Secretary included public concern over the practice of earmarking, declining balances in the Highway Trust Fund and the emergence of innovative private sector funding streams. The Secretary also cautioned that traffic tie−ups were affecting the quality of life for an increasing number of Americans and driving up housing and social costs, warning that polling data indicates there will be a future political cost. He also said that the country was reaching a tipping point when it came to dealing with growing traffic congestion and the need to add new highway and transit capacity. He said these factors together presented the Commission members with an opportunity to “substantially contribute to the future of transportation in this nation.”
Source: http://www.dot.gov/affairs/dot6506.htm

18. *May 25, Associated Press* — **Man guilty in New York bomb plot.** A Pakistani immigrant was convicted Wednesday of charges that he plotted to blow up one of Manhattan's busiest subway stations in retaliation for the Abu Ghraib prison scandal. A federal jury in Brooklyn deliberated for two days before convicting Shahawar Matin Siraj of conspiracy and other charges. He faces a maximum sentence of life in prison. Siraj and another man suspected in the plot, James Elshafay, were arrested on the eve of the 2004 Republican National Convention carrying crude

diagrams of their target −− the subway station in Herald Square, a dense shopping district that includes Macy's flagship department store. Elshafay immediately agreed to cooperate with the government.
Source: http://ebird.afis.mil/ebfiles/e20060525436535.html

19. *May 25, Associated Press* — **Thousands stranded by major rail power outage in northeast.** Power was restored Thursday, May 25, throughout the heavily traveled New York to Washington rail corridor, after a power outage stranded thousands of rush−hour commuters, stopping trains inside tunnels and forcing many passengers to get out and walk. Amtrak spokesperson Cliff Black said at about 10:30 a.m. EDT, the railroad was able to resume limited power system−wide, and shortly thereafter trains were running at full power. The outage stranded five trains in tunnels −− three NJ Transit trains, an Amtrak train in the Baltimore tunnel and another in the Hudson River tunnel. The last stalled train in the tunnels, a southbound Amtrak Acela that had just left New York, lurched back to life at 11:15 a.m. after stranding passengers for more than three hours in the heat and darkness. Amtrak does not know where the problem originated, said Black. The railroad's chairman, David Laney said the power problem "cascaded down and shut down the entire system." Black said shortly after 8 a.m. Amtrak experienced rolling power outages up and down the Northeast Corridor between Washington and Queens. NJ Transit suspended all service on its heavily traveled Northeast Corridor and North Jersey Coast lines. Midtown Direct service was diverted to Hoboken, where commuters could catch PATH trains to Manhattan.
Source: http://www.newsday.com/news/local/wire/newjersey/ny−bc−nj−−trainoutage0525may25,0,5558109.story?coll=ny−region−apnewjers ey

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

20. *May 25, Associated Press* — **Grape damage from frost widespread.** A late−April frost devastated young buds on grape vines in several western New York counties and beyond, challenging growers who had been hoping to rebound from a small crop last year. The National Grape Cooperative, which owns Welch's, estimated its New York state growers lost 30−33 percent of their grapes. The same frost painted an even bleaker picture for cooperative members in other states: Losses were estimated at 90 percent in Michigan and 75 percent in Ohio, said Jay Hardenburg, the cooperative's Eastern Region manager of member relations. The cooperative is comprised of about 1,350 growers in New York, Michigan, Ohio, Pennsylvania, Washington and Ontario. They supply all of the grapes Welch's uses for its juice, jams and jellies.
Source: http://hosted.ap.org/dynamic/stories/F/FARM_SCENE?SITE=7219&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2006−05−25−03−37−42

21. *May 25, USAgNet* — **New Zealand awarded bovine spongiform encephalopathy free status.** The World Organization for Animal Health (OIE) Wednesday, May 24, confirmed New Zealand as a bovine spongiform encephalopathy (BSE)−free country. The OIE also recognized Australia, Argentina, and Uruguay as BSE−free. Under WTO (World Trade Organization) regulations, the OIE is the internationally recognized standard−setting organization for animal health. Only Iceland and Singapore, had previously achieved official BSE−free status. New Zealand is the world's seventh largest beef exporter and exports 83 percent of the beef it produces.
Source: http://www.usagnet.com/story−national.cfm?Id=992&yr=2006

22. *May 25, Stop Soybean Rust News* — **First rust−like spores of 2006 trapped in Texas.** Syngenta has announced 30 suspected soybean rust spores caught on a slide from a Syngenta Syntinel(TM) spore trap in Beasley, TX, in Fort Bend County. Finding rust−like spores in the trap doesn't mean there's a rust infection in or even near Beasley. This is the first such report of rust−like spores captured in 2006. Syngenta said no spores were found on slides taken from three other traps located in Burleson County, TX, and in Catahoula and Franklin counties in Louisiana.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=824

[Return to top]

Food Sector

23. *May 24, U.S. Department of Agriculture* — **Research on prevention and control of E.coli in fresh produce funded.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns announced Wednesday, May 24, that USDA has awarded $1.2 million to a collaborative research effort to identify sources and risk factors of E. coli O157:H7 contamination in fresh produce. The funds will also be used to inform growers about strategies to prevent pre−harvest contamination. There have been 16 outbreaks of E. coli O157:H7 illness associated with fresh lettuce or spinach since 1995. Several of these were associated with preharvest contamination.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/05/0174.xml

24. *May 23, U.S. Food and Drug Administration* — **Turkey sandwiches recalled.** Jumbo Foods of Mukilteo, WA, is recalling 762 Smoked Turkey on Sourdough Triple Decker Sandwiches, because they have the potential to be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. The sandwiches were distributed in Washington, Oregon, and Idaho and were available at convenience stores and on military installations. No illnesses have been reported to date. The recall was the result of a routine sampling program conducted by the U.S. Army Veterinary Service which revealed that the finished product contained the bacteria.
Source: http://www.fda.gov/oc/po/firmrecalls/jumbo05_06.html

25. *May 23, U.S. Food and Drug Administration* — **Company recalls sandwiches.** Made−Rite Sandwich Company of Ooltewah, TN, is recalling approximately 27,000 chicken salad and tuna

salad sandwiches because it has the potential to be contaminated with harmful bacteria. These products are being recalled because a supplier provided an ingredient that was not processed in a manner to prevent the growth of harmful bacteria. The products have been sold under the following brands: Great American Deli, Granny Green and Lil' Cindy's. Affected product was distributed to FL, AL, MS, LA, GA, AR, TN, GA, NC, SC, VA, KY, OH, IN, MI and reached consumers through a variety of distribution avenues including retail stores, vending machines and wholesale distribution centers.
Source: http://www.fda.gov/oc/po/firmrecalls/maderight05_06.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

26. *May 25, Agence France−Presse* — **Bird flu spreads in Romania.** Bird flu continued to spread through Romania with the discovery of 11 new outbreaks including one in the south of the capital Bucharest. "Overnight Wednesday, May 24, 200 people in the fourth district of Bucharest were placed under quarantine, taking the number of isolated inhabitants in the Romanian capital to 400," Marius Dobrescu, a spokesperson for the mayor's office said. However, Romania's health ministry on Thursday, May 25, announced a nationwide "lifting of the human quarantine". Rodica Costinea, director of public health, told the media, "The slaughtering of poultry will continue, the contaminated areas will still be disinfected, but the population will be able to travel freely because there have still be no human cases in Romania." Dobrescu said quarantine would not be ended unless written instructions were received. And Nicolae Alexandri, the head of the disease prevention committee in Prahova in the center of Romania, where 10 outbreaks were reported Thursday, said all 10 areas would be placed under quarantine. In all 56 bird flu outbreaks have been discovered in Romania since the virus reemerged there 12 days ago.
Source: http://news.yahoo.com/s/afp/20060525/hl_afp/healthfluromania_060525110632;_ylt=AoC8lzWHs8jB4tEKHgOZTDKJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

27. *May 25, Agence France−Presse* — **Over 30 people quarantined in Indonesian village hit by bird flu.** More than 30 people have been asked to quarantine themselves so far in a North Sumatran village hit by bird flu outbreak, officials said. People who had close contact with any of seven relatives who have died since last month in the village are being monitored for signs of illness, World Health Organization (WHO) spokesperson Dick Thompson said. A day after another WHO spokesperson, Peter Cordingley, said the agency was stumped about the original source of the infection, Thompson said that contact with an infected bird is now considered the likely cause. The WHO has sent a 10−member team to Kubu Sembelang village, Karo District, to identify those who had close contact with the family. So far more than 30, including more relatives, have been traced and asked to quarantine themselves. Bird flu tests would be carried

out on anyone who showed signs of sickness.
Source: http://www.forbes.com/business/feeds/afx/2006/05/25/afx27722 67.html

28. *May 25, Guardian (United Kingdom)* — **Dust clouds transport bacteria from Africa around the world.** Giant clouds of dust whipped up by desert storms in Africa can carry infectious organisms to other continents, scientists claim. Despite being blown more than three miles high and exposed to radiation from the sun, strains of bacteria and fungi survived and were able to grow when they returned to Earth, researchers found. Among 40 tests of air samples taken in the mid−Atlantic, 24 revealed living microbes, including 26 colonies of bacteria and 83 fungi. They included strains capable of causing disease in humans, animals and plants. A typical gram of Sahara soil contains up to one billion bacteria, and estimates suggest two billion tons of soil particles are blown around the planet each year. Researchers used genetic tests to prove that the micro−organisms collected in the Atlantic were from specific regions in Africa. The microbes included Gordonia terra, which can cause skin disease in humans, Massaria rosatii which infects sycamore trees, and Alternaria dauci, a cause of carrot blight.
Source: http://www.guardian.co.uk/science/story/0,,1782440,00.html

29. *May 25, Boston Globe* — **Four cases of measles confirmed at Boston company.** Infectious disease trackers are moving to contain an unusual cluster of measles cases among workers at a financial services company headquartered in Boston, MA's John Hancock Tower. Four workers at Investors Bank & Trust have been diagnosed with the highly contagious respiratory illness this month. All four patients are expected to recover. Once a common scourge of childhood in the U.S., measles is now a rare condition in the developed world. The last time Massachusetts reported a cluster was in 1999, with only random, unrelated cases since then. The Boston Public Health Commission made plans to conduct an emergency round of vaccinations Thursday, May 25, for the 1,500 Investors Bank workers in the Hancock Tower. An alert was dispatched to physicians to be vigilant for other cases of the disease. Three cases are linked to a computer programmer who came from India to work for the financial firm. He had not been vaccinated against measles and became sick in early May. The men either worked directly together or conducted meetings adjacent to the computer programmer in the Hancock Tower.
Measles information: http://www.cdc.gov/nip/diseases/measles/default.htm
Source: http://www.boston.com/news/local/articles/2006/05/25/four_cases_of_measles_confirmed_at_hub_firm/

[Return to top]

Government Sector

30. *May 25, Federal Times* — **Lack of interagency contracting data frustrates OMB.** A government effort to regulate the contracting being carried out between federal agencies is hitting a snag: a lack of good data on the contracts. The lack of information is posing a big challenge to the Office of Management and Budget (OMB) as it seeks to get a better grip on interagency contracting, in which one agency sets up a contract that other agencies can use for a fee, Robert Burton, acting procurement policy administrator at OMB, said May 18. “We are spending an enormous amount of time just trying to get the data, and this is extraordinarily frustrating,” he said at the GSA Expo in San Antonio, an annual conference held by the General Services Administration from May 15 to 18. Interagency contracting has stirred concern in

Congress in recent years. OMB set up a task force last year to set better rules for using the contracts. But getting information on them has been an enormous challenge that shows the need for reforms in data collection, Burton said.
Source: http://federaltimes.com/index.php?S=1813459

[Return to top]

Emergency Services Sector

31. *May 25, Montgomery Advertiser (AL)* — **FEMA supplies arrive in Alabama.** The first deliveries of disaster relief supplies for the upcoming hurricane season have arrived in Alabama courtesy of the Federal Emergency Management Agency (FEMA). The supplies −− 57 trucks of ice in Birmingham, 6,000 tarps in Selma and hundreds of cots, blankets and hygiene kits now at Maxwell−Gunter Air Force Base −− are part of a plan to put emergency supplies at 31 two−year college campuses statewide in an unprecedented move to tap the college system for emergency shelter.
Source: http://www.montgomeryadvertiser.com/apps/pbcs.dll/article?AID=/20060524/NEWS02/605240345/1009

32. *May 25, Houston Chronicle* — **Plan seeks to smooth evacuation of special needs groups.** Officials in Texas say they've figured out a way to prevent bus caravans loaded with the Texas coast's most needy and helpless residents from wandering for hours during hurricane evacuations, as many did while fleeing Hurricane Rita in September. Under a new statewide evacuation plan, shelters will be set aside for people who evacuate cities such as Galveston in buses provided by emergency officials, said Nancy Bass, the state's mass care emergency coordinator Wednesday, May 24, during a Texas Hurricane Conference workshop on evacuation of "special needs" citizens. During Hurricane Rita, busloads of people from Galveston and Brazoria counties arrived at inland shelters only to find that other evacuees already had overwhelmed the facilities. Many people on the Galveston bus, including children, elderly, those in wheelchairs, wandered for hours in the night for shelter. This year, evacuee groups organized by local emergency management officials will be sent to shelters reserved for such groups, Bass said. The facilities will not be among those publicized as available for the general public. The so−called "point−to−point" transportation plan for special needs groups on buses is part of a massive overhaul of the state's evacuation plan since Hurricane Rita struck.
Source: http://www.chron.com/disp/story.mpl/metropolitan/3887128.htm l

33. *May 25, Government Accountability Office* — **GAO−06−808T: Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters (Testimony).** Hurricane Katrina was one of the largest natural disasters in U.S. history. The Government Accountability Office (GAO) has a body of ongoing work that covers the federal government’s preparedness and response to Hurricanes Katrina and Rita. This statement summarizes key points from GAO’s report on the military’s response to Katrina (GAO−06−643), which was issued earlier this month. It addresses (1) the support that the military provided in responding to Hurricane Katrina along with some of the challenges faced and key lessons learned; (2) actions needed to address these lessons, including GAO’s recommendations to the Secretary of Defense; and (3) the extent to which the military is taking actions to identify and address the lessons learned. In its report, GAO made several

recommendations to improve the military response to catastrophic disasters. The recommendations called for updating the National Response Plan to reflect proactive functions the military could perform in a catastrophic incident; improving military plans and exercises; improving National Guard, Reserve, and active force integration; and resolving response problems associated with damage assessment, communication, search and rescue, and logistics issues. The Department of Defense partially concurred with all of the recommendations.
Highlights: http://www.gao.gov/highlights/d06808thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−808T

34. *May 24, Air Force Link* — **Department of Defense officials defining roles for disaster response.** With hurricane season nearing, the Department of Defense (DoD) has tremendous assets to offer a civilian−led response to a major disaster, said a top DoD official involved in the process. "Those assets are ready for deployment, and...we are better prepared than at any point in our nation's history to move that assistance as rapidly as is humanly possible," said Paul McHale, assistant defense secretary for homeland defense. DoD defense coordinating officers will be assigned full−time to each of the Federal Emergency Management Agency's (FEMA) 10 regional offices to ensure coordinated planning and operational integration among DoD, the Department of Homeland Security and FEMA. In addition, DoD can offer aviation assets capable of providing near−real−time damage assessments, McHale said.
Source: http://www.af.mil/news/story.asp?id=123020790

35. *May 24, Associated Press* — **Two−day hurricane drill reveals flaws in Louisiana's emergency response system.** While new communications equipment provided by the state worked well, Louisiana's two−day hurricane drill designed to identify flaws in the state's emergency response system did just that. It highlighted needs for additional training for those involved in handling national incidents, more computers at the state emergency operations center and large visual displays allowing everyone to get information at the same time. Improvement also is needed in communications among various agencies and with the media. Among the drill's successes was the new communications equipment purchased by the state. The mobile, self−contained systems allow first responders to communicate with each other if there is a disaster. In addition, a big improvement was the coordination between the city of New Orleans and state agencies. While exercises Tuesday, May 23, focused largely on evacuation and sheltering, the Wednesday, May 24, drill dealt largely with officials' ability to respond after a hurricane makes landfall, when power and telephone lines go down, trees block roadways and communications systems often become hampered.
Source: http://www.sunherald.com/mld/sunherald/14658105.htm

36. *May 24, Associated Press* — **White House staff holds hurricane exercise.** President Bush's Cabinet tested its readiness and response to a catastrophic hurricane Wednesday, May 24, during a desktop drill carried in the nation's capital. "This was a 'roll−up−your−sleeves' session in which participants dealt with difficult decisions and had frank discussions about the best way to deal with a catastrophic hurricane," White House spokesperson Ken Lisaius said. He said the participants dealt with evacuation and shelter plans, communications, reporting structures for disaster managers and coordination from Washington.
Source: http://www.forbes.com/work/feeds/ap/2006/05/24/ap2771886.htm l

37.

May 24, Associated Press — **Florida EOC moved to alternate location for mock storm, terror drill.** A simulated terrorist attack Wednesday, May 24, in Tallahassee, FL, and mock Hurricane Zoey hitting near Tampa tested the ability of the state to move its emergency operation to another location −− the National Guard's Camp Blanding. The exercise was designed to test the ability of emergency managers from all phases of state and federal government to work together to meet the demands of a disaster −− outside the comfortable confines of the state's emergency operation center (EOC) in Tallahassee. The exercise began Friday, May 19, and wrapped up Thursday, May 25.
Source: http://www.bradenton.com/mld/bradenton/news/breaking_news/14 657086.htm

[Return to top]

Information Technology and Telecommunications Sector

38. *May 25, IDG News Service* — **New World Cup worm in circulation.** World Cup soccer fans should be aware of a new worm being circulated by e−mail with the German−language message "WM−Tickets" or "Weltmeisterschaft," security vendor Sophos warned Wednesday, May 24. The e−mail contains an attachment, which, when opened, activates the W32/Zasran−A worm. The worm is programmed to send itself to addresses stored in Microsoft's Outlook address book and manipulate security settings to give hackers access to other personal information stored in users' PCs. The Zasran−A worm is the second World Cup−related virus detected in May, with the games scheduled to kick off Friday, June 9.
Source: http://www.networkworld.com/news/2006/052506−world−cup−new−w orm−tries.html

39. *May 24, Security Focus* — **Cisco VPN Client local privilege escalation vulnerability.** Cisco VPN Client is susceptible to a local privilege escalation vulnerability. This issue is due to an unspecified flaw in the VPN client GUI application. Analysis: The issue is due to an unspecified flaw in the VPN client GUI application which allows local attackers to gain Local System privileges on affected computers. This facilitates the complete compromise of affected computers.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18094/info
Solution: Cisco has released an advisory along with fixes to address this issue: http://www.securityfocus.com/archive/1/434934
Source: http://www.securityfocus.com/bid/18094/discuss

40. *May 24, VNUNet* — **Botnet floods UK firms with 250 million spams.** A botnet of more than 150,000 compromised PCs was responsible for subjecting UK businesses to a flood of more than 250 million spam e−mails last weekend. Security services company BlackSpider Technologies said that the spam deluge began over the weekend and peaked on Monday, May 22. The e−mails are still being distributed by the botnet, according to BlackSpider, but in fewer numbers. Although the content of the e−mails varied, each one contained a link to one of several Websites selling "pharmaceutical" products. The subject lines and body text contained obfuscated names of drugs, ending with a poem or paragraph of random obfuscating words. Refer to source for an example.
Source: http://www.vnunet.com/vnunet/news/2156823/botnet−floods−uk−f irms−250

41. *May 24, Sophos* — **Da Vinci Code spam hits e−mail inboxes.** Anti−spam experts at Sophos are calling on consumers to be wary of unsolicited e−mails trying to sell them goods via spam, as an unsolicited e−mail campaign offers a copy of Dan Brown's best−selling novel, "The Da Vinci Code." Sophos has intercepted e−mails inviting recipients to join a book club, claiming to offer a free copy of "The Da Vinci Code" as an incentive. The e−mail calls on people to "Read the novel everyone's STILL talking about" and to "Get the Da Vinci Code free, plus five more bestsellers for 99 cents." Refer to source to view a screen shot of the Da Vinci Code e−mail.
Source: http://www.sophos.com/pressoffice/news/articles/2006/05/davi nci.html

42. *May 24, Government Computer News* — **NIST publishes draft report on PIV card.** The National Institute of Standards (NIST) has released a draft report detailing requirements and specifications for smart cards and readers that agencies can use when purchasing products to meet upcoming Homeland Security Presidential Directive 12 deadlines. The report offers interoperability standards and performance−based requirements for Personal Identity Verification (PIV) systems consistent with mandates under Federal Information Processing Standard 201−1.
NIST Special Publication 800−96: http://csrc.nist.gov/publications/drafts/800−96/Draft−ipd−sp 800−96−052306.pdf
Source: http://www.gcn.com/online/vol1_no1/40857−1.html

43. *May 22, Associated Press* — **Computer outage strikes Montana government.** Much of Montana's government computer system crashed Monday, May 22. The vast majority of services and computers remained down, and state government was essentially immobilized, said Dick Clark, the state's chief information officer. Clark said he couldn't speculate if a virus or hacker was to blame. Clark said the state government saw similar problems about four years ago when a virus brought the network down.
Source: http://seattlepi.nwsource.com/business/1700AP_Computer_Outag e.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 is currently researching a zero−day vulnerability in Microsoft Word. In order for this exploit to be carried out, a user must first open a malicious Word document attached to an email or otherwise provided to them by an attacker. When the document is opened, malicious code is installed on the user's machine. The exploit then attempts to connect to a remote host. US−CERT and Microsoft will continue to investigate the public reports to help provide additional guidance as necessary. There is currently no patch available for this vulnerability.

For more information please review the following:

TA06−139A Microsoft Word Vulnerability:
http://www.us−cert.gov/cas/techalerts/TA06−139A.html

VU#446012 Microsoft Word buffer overflow: http://www.kb.cert.org/vuls/id/446012

Cyber Security Tip: http://www.us−cert.gov/cas/tips/ST04−010.html

Microsoft Security Advisory (919637):
http://www.microsoft.com/technet/security/advisory/919637.ms px#EAF

US−CERT recommends the following actions to mitigate the security risks:

Install anti−virus software, and keep its virus signature files up to date

Block executable and unknown file types at the email gateway

US−CERT strongly encourages Federal Agencies to educate their user base and constituency about the risk of opening unknown attachments from unknown sources even if sent by a known and trusted source.

We will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 38566 (−−−), 445 (microsoft−ds), 25 (smtp), 12106 (−−−), 7200 (fodms), 49200 (−−−), 41170 (−−−), 50497 (−−−) 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

44. *May 24, Associated Press* — **Stairwell fire forces evacuation of Philadelphia City Hall.** Fire broke out in a stairwell at Philadelphia's City Hall on Wednesday, May 24, causing extensive water damage in the historic building and forcing the evacuation of about 500 people. Firefighters responded around 9:30 a.m. EDT and found heavy smoke on the third and fourth floors. They traced the smoke to a trash fire under a stairwell between the second and third floors, said Daniel Williams, executive fire chief.
Source: http://www.phillyburbs.com/pb−dyn/news/103−05242006−661043.h tml

[Return to top]

General Sector

Nothing to report.
[Return to top]