Department of Homeland Security Daily Open Source Infrastructure Report for 04 November 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- The Associated Press reports that Los Angeles International Airport will be among 15 facilities to receive new technology aimed at averting potential airfield collisions. (See item 8)

- The Boston Globe reports that a quarantine station is being built at Boston's Logan International Aiport to allow staff from the U.S. Centers for Disease Control and Prevention to evaluate the health threats posed by incoming travelers. (See item 20)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

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. *November 03, Hartford Courant (CT)* — **Spent nuclear fuel pool leaked.** Radioactive water from the decommissioned Connecticut Yankee nuclear plant's spent fuel pool once leaked into the surrounding soil, the Nuclear Regulatory Commission (NRC) reported Wednesday, November 3. The contamination appears to have remained on−site, and public health and safety is not endangered, both the NRC and Connecticut Yankee officials said. Workers decommissioning the plant Monday, October 31, discovered hairline cracks in the six−foot thick concrete walls containing the spent fuel pool, NRC spokesperson Neil Sheehan said. Those cracks may not have been the reason for the contamination. Instead, it appears an

unknown quantity of contaminated water seeped through seams in the concrete into a small area of soil, according to Connecticut Yankee officials. The spent fuel pool housed the nuclear plant's highly radioactive uranium pellets for decades. The rods and radioactive metals have been removed from the pool, but the water remains. The Haddam Neck, CT, plant, which permanently shut down in 1996, produced 110 billion kilowatt hours of electricity over 28 years.
Source: http://www.courant.com/news/local/hc−nukeleak.artnov03,0,412 8957.story?coll=hc−headlines−local

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *November 03, Tampa Tribune (FL)* — **Broken gas line in Florida prompts evacuations.** A gas line break on River Gulf Road in Port Richey, FL, prompted city police to evacuate residents and business owners Wednesday afternoon, November 2, fire officials said. The gas leak, which occurred about 2 p.m. EST, was caused by workers from U.S. Water Co. who were digging on the road, according to Capt. Rob Gupton of the Port Richey Fire Department. Residents of a nearby mobile home park and several businesses were evacuated. Police cordoned off both ends of the road with yellow tape as crews from Clearwater Gas System worked to contain the gas leak and repair the broken line. No one was injured and the evacuations were done as a precaution, Gupton said.
Source: http://tampatrib.com/pasconews/MGB9OEGHKFE.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *November 03, CNET News.com* — **Adware maker was blackmailed by cybergang.** Advertising software maker 180solutions on Wednesday, November 2, said it was the target of a scheme to extort money by Dutch cybercriminals and is helping in the case against them. Dutch police in early October arrested three individuals suspected of commandeering about 1.5 million PCs using a Trojan horse. They allegedly used the network of so−called zombie PCs to steal credit card numbers and other personal data, and to blackmail online businesses. Authorities had not disclosed which online businesses had been targeted in the blackmail schemes. 180solutions on Wednesday came forward and identified itself as one of the victims and said it helped gather evidence against one of the three suspects. One of the three arrested men was a distributor of 180solutions' software, said Sean Sundwall, a 180solutions spokesperson. The suspect got involved with botnets, or networks of hijacked computers, to install the adware, moving 180solutions to stop payments to the individual. "We shut him off and he asked to be reinstated," Sundwall said. When he was not, the individual threatened with

a denial of service attack unless 180solutions paid him an undisclosed sum. "The attack ensued in early August and that is when we involved the FBI," Sundwall said.
Source: http://news.com.com/Adware+maker+We+were+victims+of+cybergang/2100−7349_3−5930099.html?tag=nefd.top

4. *November 03, Department of the Treasury* — **Treasury action targets Southeast Asian narcotics traffickers.** The Department of the Treasury's Office of Foreign Assets Control (OFAC) on Thursday, November 3, identified 11 individuals and 16 companies that are part of the financial and commercial network of designated significant foreign narcotics trafficker Wei Hsueh−kang and the United Wa State Army (UWSA). The names were added to OFAC's Specially Designated Nationals and Blocked Persons list pursuant to the Foreign Narcotics Kingpin Designation Act. "Wei and the UWSA's opium trafficking plagues the society and economy of Southeast Asia. We're acting to protect the U.S. financial sector from this network's tainted drug profits, as well as ensure Wei and his cohorts can't use the American financial system to move or launder their opium proceeds," said Robert Werner, OFAC Director. The UWSA is the largest and most powerful drug trafficking organization in Southeast Asia. Among the key financial individuals designated by OFAC on Wednesday are Warin Chaichamrunphan and Winai Phitchaiyot. They act for or on behalf of Wei and the UWSA in various front companies, and assist in narcotics trafficking activities. This action freezes any assets found in the United States and prohibits all financial and commercial transactions between the designated persons and entities and any U.S. person.
Source: http://www.treasury.gov/press/releases/js3009.htm

5. *November 02, USA Today* — **Cyber crooks break into online accounts with ease.** Many consumers and small−business owners believe online transactions are safe if they use a firewall, keep anti−virus software updated and follow security tips posted on banking Websites. Not so, Internet security experts and federal regulators say. "What banks don't tell you is how easy it is to bypass those protections, and how prolific the threat is, because then you wouldn't do online banking," says Peter Vogt, a board member of Information Systems Security Association, an international group of tech security professionals. To gain access to most online bank accounts, you only need a user name and a password, however, Bank of America plans to require extra log−on steps for all Internet customers by early next year, becoming the first major U.S. bank to add another level of authentication. While financial industry executives acknowledge the Internet's security pitfalls, they say they have been mindful of minimizing risks to consumers and small businesses. Consumer financial fraud has been around a long time, but e−commerce has opened new criminal frontiers. "In the past, everything was much more traceable. Now you can open 10,000 (bogus) accounts in the time it used to take to open one, all in a faceless Internet," says Gartner banking analyst Avivah Litan.
Source: http://www.usatoday.com/money/industries/technology/2005−11−02−cybercrime−online−accounts_x.htm

6. *November 02, Computing* — **UK bank readies online user authentication.** UK bank HSBC will issue keyring−sized authentication devices to UK Internet banking customers if phishing e−mails and key−logging software continues to grow. The bank, which has seen a 50 percent increase in Internet banking use in the last year, believes it has strong enough security measures in place to stem the rise in online identity theft, but is ready to issue personal security devices if needed. HSBC has already piloted two−factor authentication devices in Hong Kong and Brazil,

but wants to tackle Internet crime through consumer education and anti−fraud detection technologies before deploying them in the UK. ‘There is a trade−off between security and convenience,” said Joe Garner, general manager of customer propositions and head of personal financial services at HSBC. “We are confident that the security measures we have in place today give the highest levels of security. But if we do see an escalation of online crime then we have a tried and trusted solution that we can deploy,” said Garner.
Source: http://www.computing.co.uk/computing/news/2145388/hsbc−readi es−online−user

[Return to top]

Transportation and Border Security Sector

7. *November 04, Government Accountability Office* — **GAO−06−145: Amtrak Management: Systemic Problems Require Action to Improve Efficiency, Effectiveness, and Accountability (Report).** Amtrak has struggled since its inception to earn sufficient revenues and operate efficiently. In June 2002, Amtrak’s new president began major efforts to improve efficiency. However, the financial condition of the company remains precarious, requiring a federal subsidy of more than $1 billion annually. Capital backlogs are now about $6 billion, with over 60 percent being attributable to its mainstay Northeast Corridor service. The Government Accountability Office (GAO) reviewed Amtrak’s (1) strategic planning, (2) financial reporting and financial management practices, (3) cost containment strategies, (4) acquisition management, and (5) accountability and oversight. GAO makes recommendations in all five areas reviewed. These are designed to improve the strategic planning process, improve financial information, strengthen controls over costs and acquisition of goods and services, and strengthen transparency, accountability, and oversight. GAO also suggests that Congress ensure that future legislation for intercity passenger rail service contains clear goals and stakeholder roles, and incentives for results and accountability. Department of Transportation officials, in general, agreed with the report’s findings. Amtrak’s president was not convinced GAO’s recommendations would achieve the results GAO expects but, in general, did not comment on specific recommendations.
Highlights: http://www.gao.gov/highlights/d06145high.pdf
Source: http://www.gao.gov/new.items/d06145.pdf

8. *November 03, Associated Press* — **Los Angeles International Airport to get improved ground radar system.** Los Angeles International Airport (LAX), which has one of the nation's highest rates of runway safety violations, will be among 15 facilities to receive new technology aimed at averting potential airfield collisions, federal officials said Wednesday, November 2. The new ground radar system will help prevent planes from getting too close to one another by giving air traffic controllers precise information about their locations on the airfield. The system should be operating at LAX sometime next year. "This will be a much more powerful set of eyes for controllers to see things that now can't be seen and to identify specifically what they are," said Donn Walker, a Federal Aviation Administration spokesperson. LAX ranked sixth among the nation's 25 busiest commercial airports for runway safety violations between October 1, 2004, and September 30, 2005, newly released statistics show. LAX's existing ground radar system displays objects as blobs on a monochromatic screen and doesn't distinguish between a person, a vehicle and an aircraft. The new technology −− Airport Surface Detection Equipment, Model X, or ASDE−X −− will show that an object is an aircraft and

identify the airline and flight number.
Source: http://www.mercurynews.com/mld/mercurynews/news/breaking_new s/13069602.htm

9. *November 03, Associated Press* — **Transportation Security Administration plans to expand "registered traveler" program.** The Transportation Security Administration (TSA) plans to make a "registered traveler" program available nationwide, agency chief Kip Hawley said Thursday, November 3, in prepared testimony to Congress. The initial rollout is scheduled for June 20. The program, which was tested at five airports, allows people to avoid random pat−downs if they pay a fee, clear a voluntary background check and provide some form of biometric identification, like a fingerprint. It's designed to let people who travel often avoid delays and to free up screeners to focus on other travelers. Hawley said the TSA is considering adding benefits to the program, such as letting registered travelers keep their shoes and their jackets on, or setting up special screening lanes. The government will conduct the background checks but Hawley said the plan is to use private companies to enroll travelers, issue ID cards that would be shown at airports and promote the program. In January, TSA plans to issue guidance on collecting and storing biometric data and to unveil an appeals process for people who are rejected as registered travelers.
Source: http://seattlepi.nwsource.com/national/1155AP_Passenger_Scre ening.html

10. *November 02, KOMO 4 News (WA)* — **Immigration agents arrest 105 suspected illegal workers.** Federal immigration agents arrested 105 suspected illegal workers Wednesday, November 2, at warehouses operated by Regal Logistics Corp. in the Tacoma suburb of Fife, WA, officials said. The workers were identified after Immigration and Customs Enforcement agents audited recent hiring records of Phoenix Staffing LLC and found what the federal agency termed "discrepancies leading agents to believe that a number of the company's employees may not have been authorized to work in the United States." Phoenix Staffing is a temporary employment agency used by Regal Logistics. Regal Logistics stores merchandise entering the United States from other countries, the agency added. According to its Website, Regal Logistics manages "warehousing, transportation and distribution for the toy, apparel, houseware and footwear industries." Immigration agents said the majority of the unauthorized employees were from Mexico and it appeared many used counterfeit IDs to obtain the jobs. Wednesday's inspection was part of an effort to focus on businesses with ties to "security sensitive sites and critical infrastructure facilities" such as airports, military bases and customs warehouses. Unauthorized workers with access to such sites can be exploited by terrorists or smugglers. Regal Logistics' facilities are close to major seaports, railyards and airports in the Seattle−Tacoma area.
Source: http://komonews.com/news/story.asp?ID=40060

11. *November 02, Time Magazine* — **Virgin Airlines buys Tamiflu.** Richard Branson, Chairman of Virgin Group Ltd. said Wednesday, November 2, that his company is looking into machines and new technologies to put on aircrafts to kill germs in anticipation of a bird flu pandemic. He said his company has purchased 10,000 doses of the drug Tamiflu for his staff. In response to questions about companies hording Tamiflu, Branson said, "We've bought [Tamiflu] because our staff is on the front line." Branson also said that despite Virgin's best efforts to protect staff and passengers, if the flu starts spreading person to person, "it will most certainly affect the airline industry."
Source: http://time.blogs.com/global_health/2005/11/richard_branson. html

[Return to top]

Postal and Shipping Sector

12. *November 03, Global Security Newswire* — **Installation of anthrax detectors at postal facilities nears end.** The United States Postal Service is nearing completion of a four−year project to install systems that can detect anthrax in the mail. By the beginning of December, the Postal Service expects to have installed Biohazard Detection Systems at 282 mail−processing facilities around the country, said Don Crone, USPS manager of mail−processing protection systems. These detection systems are the Postal Service's front−line defense against an anthrax attack through the mail system. Crone said the system has so far proven to be perfectly reliable. He said 27 billion pieces of mail have been screened without a single false positive. If a system were to detect anthrax, the facility would be evacuated and the Department of Homeland Security and the Centers for Disease Control and Prevention would be notified immediately. The sample that tested positive for the pathogen would be retested. If the result were positive, all employees present at the facility or who had contact with the infected batch of mail would be put on a five−day regimen of the anti−anthrax drug Cipro. Crone claimed the Biohazard Detection System is the most advanced system for detecting anthrax transported through the mail in the world.
Source: http://www.nti.org/d_newswire/issues/2005_11_3.html#9F23F5F2

[Return to top]

Agriculture Sector

13. *November 03, Billings Gazette (MT)* — **Horses come down with pigeon fever.** Three of Jan Britton's horses living near Shepherd, MT, have contracted pigeon fever, a disease that used to be confined to California but has spread across the West. Pigeon fever is so named because infected animals often develop abscesses in their chests that swell. Shepherd area veterinarian Vicki Bokum said pigeon fever hit Yellowstone County last year and she had to euthanize one horse that was sick. The disease can become fatal if it infects internal organs such as the kidneys, liver and spleen. This fall, she's seen cluster cases mostly in the Shepherd area and around Yellowstone County. The pigeon fever bacteria is hardy and can be spread by flies, birds, or contaminated objects such as halters or buckets. According to Colorado State University, the infectious bacteria can live up to 55 days in the soil, bedding or manure. But that's not what many area vets are seeing. Isolated clusters are popping up apparently with no obvious carrier.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2005/11/03/build/local/30−horse−fever.inc

14. *November 03, Casper Star Tribune (WY)* — **Chronic wasting disease moves west.** State and now tribal game managers have detected three new cases of chronic wasting disease (CWD) in Wyoming. The new locations are in the Owl Creek drainage, north and west of Thermopolis. The disease had not previously been detected in this area. On Friday, October 28, the Wyoming Game and Fish Department announced that two mule deer bucks, taken just north by northwest

of Thermopolis in the lower Owl Creek drainage, had tested positive for the disease. On Wednesday, November 2, the Shoshone and Arapaho Fish and Game Department announced that a whitetail buck, taken one mile east of the Arapaho Ranch headquarters, had also tested positive. The case on the reservation, about 20 miles due west of Thermopolis, is the most western case in the state. Game and Fish Deputy Director Gregg Arthur directed Game and Fish personnel in the Cody region to remove up to 50 deer within a five−mile radius of where the two Thermopolis−area deer were killed.
CWD information: http://www.cwd−info.org/
Wyoming Game and Fish Department statement:
http://gf.state.wy.us/services/news/pressreleases/05/10/28/0 51028_1.asp
Source: http://www.casperstartribune.net/articles/2005/11/03/news/wyoming/ca716c7b34efcf34872570ae0008412f.txt

15. *November 03, Mercosur (Uruguay)* — **Brazil confirms more foot−and−mouth diseae outbreaks.** Brazil confirmed the existence of ten new outbreaks of foot−and−mouth disease concentrated in a county of the state of Matto Grosso do Sul where the epidemic started in early October. Jorge Caetano head of the Ministry of Agriculture Livestock Health department confirmed that the new outbreaks are all in Eldorado, an area under quarantine surrounded by a sanitary ring with military support. The area which Brazilian sanitary officials have defined as "tampon" covers 12 square miles and has been clearly marked since early October. An estimated 20,000 head of cattle are in the area, of which 1.900 have already been slaughtered. The Livestock Health Department and Matto Grosso do Sul officials are assessing how many more animals have to be culled to prevent further contagion. Brazil which was the world's leading beef exporter last year with 2.4 billion U.S. dollars is now facing a ban from almost fifty countries, following the outbreaks.
Source: http://www.mercopress.com/Detalle.asp?NUM=6695

16. *November 02, Illinois Department of Agriculture* — **Illinois veterinarians prepare to manage disease outbreaks.** Nearly 100 Illinois veterinarians will continue training and learn to execute emergency management plans designed to contain animal diseases, Friday, November 4, in Springfield, IL. The training is part of the Illinois Department of Agriculture's (IDOA) IVERT (Illinois Veterinary Emergency Response Team) initiative, an effort to establish a unified response to animal health emergencies by increasing intergovernmental cooperation and building a partnership between animal health officials and private practitioners. This is the third statewide IVERT training session administered by IDOA. Previous sessions have included instruction on the identification of foreign animal diseases, potential bioterrorist agents, the Incident Command System (ICS) that state and federal emergency management agencies use when responding to disasters and hands−on exercises that allow veterinarians to apply the lessons they have learned in a simulated animal disease outbreak. This year's session will include an FBI perspective on the threat of agroterrorism and discussions on animal diseases, particularly foot and mouth disease and avian influenza.
Source: http://www.agr.state.il.us/newsrels/r1102051.html

[Return to top]

Food Sector

17. *November 03, Reuters* — **European Union authorizes imports of genetically modified maize for use in feed.** The European Union (EU) has authorized imports of a genetically modified (GM) maize, the fifth new GM approval since the EU ended its informal biotech ban last year, the bloc's executive Commission said on Thursday, November 3. The maize, modified to resist certain insects and herbicides, will be used in animal feed. The authorization is valid across the EU−25 for 10 years. The EU decision is a rubberstamp procedure applied by the Commission. It is permitted under a legal default process that kicks in when ministers are unable to agree among themselves after a period of three months. Despite last year's lifting of an effective biotech moratorium using default procedures, EU countries have not managed to agree by themselves on a GM approval since 1998.
Source: http://abcnews.go.com/US/wireStory?id=1276887

18. *November 02, Food Safety and Inspection Service* — **Food Safety and Inspection Service announces quick and efficient method of detecting E. coli.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) Wednesday, November 2, announced that it is adopting the BAX system to detect Escherichia coli O157:H7 in raw beef. The BAX system has proven to be a rapid, highly sensitive test for the detection of low levels of E. coli O157:H7 in raw beef products and FSIS will use it as an initial screening test for all raw beef samples that are analyzed for E. coli O157:H7. Any sample found positive by a screening test must then undergo further confirmatory analysis. The same system is currently in use by FSIS for the detection of Salmonella and Listeria monocytogenes. The BAX system will substantially reduce the number of samples that are initially found to be a screening positive, but then later confirmed to be negative. By reducing the number of false screening−positives, FSIS will save critical laboratory resources that can be used for other food safety or food defense testing. The improved screening test also reduces the number of days that raw product from negative production lots must be held pending laboratory results. FSIS is optimistic this will increase the number of establishments that choose to hold product pending FSIS sampling results.
Source: http://www.fsis.usda.gov/News_&_Events/NR_110205_01/index.as p

[Return to top]

Water Sector

19. *November 03, Naples News (FL)* — **Hurricane damage costs water district $18 million.** A few hours of severe weather caused by Hurricane Wilma will cost the South Florida Water Management District $18 million. The financial impact could affect projects the district has under way, such as the C−43 reservoir for the Caloosahatchee River and plans to accelerate the cleanup of Lake Okeechobee. Water Management District spokesperson Kurt Harclerode said it's too early to tell when or if the district will postpone projects as a result of the unexpected loss. Affected projects could include Comprehensive Everglades Restoration projects and Acceler8 projects. Acceler8 projects include the C−43 reservoir, which will provide storage for excess water flows to the Caloosahatchee River. The storm ripped underwater vegetation from Lake Okeechobee and tore out plants in water treatment areas that clean water before it reaches the Everglades. Winds also damaged nearly all of the district field stations. Harclerode said the district has to remove downed trees and other debris from its miles of canals. He said there is enough debris in the canals to fill the Orange Bowl in Miami three times.
Source: http://www.naplesnews.com/npdn/news/article/0,2071,NPDN_1494

0_4207501,00.html

[Return to top]

Public Health Sector

20. *November 03, Boston Globe (MA)* — **Quarantine station to open at Logan airport.** With the threat of bioterrorism and infectious diseases growing, the federal government by the end of this year plans to open a quarantine station at Boston, MA's Logan International Airport where officials can evaluate the health threats posed by incoming travelers. The Massachusetts Port Authority, which operates Logan, is building an office suite and an isolation room where a five−person staff from the U.S. Centers for Disease Control and Prevention (CDC) can evaluate travelers and train airport and airline personnel on how to detect symptoms consistent with infectious diseases. The CDC office will be located in the international Terminal E. Maria Pia Sanchez, officer in charge for the CDC at Logan, said she and her staff will monitor all international arrivals at Logan. CDC officials say a quarantine station will not have a major impact on most travelers arriving from abroad at Logan, since a tiny percentage are actually pulled aside for evaluation. But if avian flu were to mutate into a fast−spreading human virus or a bioterrorism attack occurred, quarantine stations like the one in Boston would probably play a much more aggressive role, serving as the nation's first line of defense in containing the threat.
CDC Division of Global Migration and Quarantine: http://www.cdc.gov/ncidod/dq/mission.htm
Source: http://www.boston.com/business/healthcare/articles/2005/11/03/quarantine_station_to_open_at_logan/

21. *November 03, Howard Hughes Medical Institute* — **Proteins take on new roles in malaria parasite.** While searching for new targets for malaria drugs and vaccines, a team including a Howard Hughes Medical Institute (HHMI) medical student fellow reached a fundamental insight about evolution: different species make use of similar sets of proteins in different ways. “We've observed that organisms may share many similar proteins and yet retain very little parallel function among them,” said Taylor Sittler, a medical student at the University of Massachusetts Medical School. “For instance, Plasmodium falciparum −− the parasite that causes malaria −− shares with its human host many proteins involved in forming chromosomes during cell division, but those proteins may interact in different ways, creating different cellular pathways and even entirely different functions. This contradicts the currently accepted paradigm that shared proteins interact simply because their genes are conserved.” The discovery showcases the burgeoning power of proteomics, the systematic study of proteins. If the genes of an organism comprise its blueprint, then proteins are the building materials. By comparing proteins in different organisms, researchers can identify each protein within cellular pathways. In the case of disease−causing organisms, this can lead to new ideas about how to disarm the pathogen.
Source: http://www.hhmi.org/news/sittler.html

22. *November 03, Russian News & Information Agency* — **Russian Agricultural Ministry gives update on bird flu.** The Russian Agriculture Ministry said Thursday, November 3, that bird flu had been confirmed in 12 Russian villages and that 20 more could be contaminated. The disease has been registered in a village in the Omsk region and in three villages in the Altai Territory, both in Siberia. Another is suspected of contamination in Altai. Two villages were hit

in the Chelyabinsk region, and three in the Kurgan region (both in the Urals), with four more areas suspected of an outbreak. Two villages have been infected in the central Russian region of Tambov, about 250 miles southeast of Moscow and one village has the disease in the Tula region, about 120 miles south of the Russian capital. Sixteen villages in the Siberian Novosibirsk region could also have instances of bird flu.
Source: http://en.rian.ru/russia/20051103/41984698.html

23. *November 03, Reuters* — **Flu pandemic risks sparking global recession.** A bird flu pandemic risks triggering a global recession, the Asian Development Bank (ADB) said on Thursday, November 3. The ADB said a year−long shock from bird flu in humans would cost Asian economies as much as $283 billion and would reduce the region's gross domestic product by 6.5 percentage points, hitting the trading hubs of Hong Kong and Singapore the hardest. "Avian flu presents a major potential challenge to the development of the region, perhaps the most serious since the financial crisis of 1997," said the ADB. "A pandemic will likely slow or halt economic growth in Asia and lead to a significant reduction in trade, particularly of services. In the long run, potential economic growth will be lower and poverty will increase." The World Bank, in its twice−yearly report on East Asia's economies, said on Thursday, November 3, avian flu was a big risk to growth in 2006 due to potential policy actions such as quarantines and travel restrictions.
ADB report: http://www.adb.org/Documents/EDRC/Policy_Briefs/PB042.pdf
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=scienceNews&storyID=2005−11−03T164022Z_01_SIB260908_RTRIDST_0_SCIENCE−BIRDFLU−DC.XML&archived=False

24. *November 02, Food and Drug Administration* — **Food and Drug Administration announces the use of electronic drug labels.** In a continuing effort to use modern information technology to help inform the public and health care providers and to further improve patient safety, the Food and Drug Administration (FDA) Wednesday, November 2, began requiring drug manufacturers to submit prescription drug label information to FDA in a new electronic format. This electronic format will allow healthcare providers and the general public to more easily access the product information found in the FDA−approved package inserts (labels) for all approved medicines in the U.S. These new electronic product labels will be the key element and primary source of medication information for "DailyMed" −− a new interagency online health information clearinghouse that will provide the most up−to−date medication information free to consumers, healthcare providers and healthcare information providers. Under regulations that became effective Wednesday, November 2, drug manufacturers are now required to submit to FDA prescribing and product information (i.e., the package insert or label) in a structured product labeling (SPL) format that provides accurate, up−to−date drug information using standardized medical terminology in a readable, accessible format.
DailyMed: http://dailymed.nlm.nih.gov
Source: http://www.fda.gov/bbs/topics/NEWS/2005/NEW01252.html

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

25. *November 02, Government Accountability Office* — **GAO−06−235T: Hurricanes Katrina and Rita: Contracting for Response and Recovery Efforts (Testimony).** The devastation experienced by those throughout the Gulf Coast in Louisiana, Mississippi, Alabama, and Texas in the wake of Hurricanes Katrina and Rita has called into question the government's ability to effectively respond to such disasters. The government needs to understand what went right and what went wrong, and to apply these lessons to strengthen its disaster response and recovery operations. The federal government relies on partnerships across the public and private sectors to achieve critical results in preparing for and responding to natural disasters, with an increasing reliance on contractors to carry out specific aspects of its missions. At the same time, the acquisition functions at several agencies are on the Government Accountability Office's (GAO) high risk list, indicating a vulnerability to fraud, waste, abuse, and mismanagement. GAO was asked to provide an overview of (1) its role in evaluating the contracting community with regard to disaster preparedness and response; (2) GAO's plans for reviewing the performance of the federal government and its contractors in preparing for and responding to the hurricanes; and (3) what GAO has learned so far about the performance of the federal government and its contractors in preparing for and responding to the hurricanes.
Highlights: http://www.gao.gov/highlights/d06235thigh.pdf
Source: http://www.gao.gov/new.items/d06235t.pdf

26. *November 02, Federal Computer Weekly* — **Progress being made in radio communications for first responders.** Significant progress has been made in the past year in creating standards for interoperable radio communications for first responders, a top federal communications official said Wednesday, November 2. "For the first time, we're able to say things are changing, things are moving," said Dereck Orr, program manager of the Office of Law Enforcement Standards at the National Institute of Standards and Technology. Orr spoke during a panel discussion on interoperable communications at the Technologies for Critical Incident Preparedness Conference and Exposition, which is sponsored by the Department of Homeland Security and Department of Justice. In October, Project 25 (P25), a public/private partnership to create standards for interoperable radio communications, adopted a fixed station interface and a console interface, Orr said. Public safety agencies are already starting to reference the standards in their procurement requests, and vendors are building new products to meet the standards, he said. A third standard, the Inter RF Subsystem Interface (ISSI), is on track for adoption by March 2006, Orr said. The ISSI is one of the most important standards because it allows different jurisdictions to interoperate, he said. All three standards will be complete by the end of 2006, according to Orr.
Technologies for Critical Incident Preparedness Conference and Exposition Website: http://www.regonline.com/eventinfo.asp?EventId=21494
Source: http://www.fcw.com/article91287−11−02−05−Web

27. *November 02, West Virginia Gazette* — **City, county to unite emergency−management offices in West Virginia.** Officials in Kanawha County and Charleston, WV, expect a new public−safety partnership will begin a new age of emergency planning cooperation. The new Metro Emergency Management Authority (MEMA), unveiled Wednesday, November 2, will

take away some of the autonomy of the city’s and county’s emergency services directors and will mandate them to work together on emergency planning, according to a copy of the plan. The plan still must be approved by Charleston City Council, Kanawha County commissioners and the Metro 911 board, but organizers expect support from those groups. The director of Charleston’s Office of Emergency Services and Homeland Security and Kanawha County’s emergency services director will serve as each other’s deputy director starting in December, County Commission President Kent Carper said.
Source: http://wvgazette.com/section/News/2005110118

28. *November 02, Associated Press* — **Texas Governor's office updating homeland security plan.** As part of its latest homeland security plan, Texas is creating a new intelligence center to sift through information gathered by the state's 2,685 police departments to detect possible terrorism patterns and to enhance law enforcement. "A lead in a small town in Texas can have statewide, national or international significance," the Texas Homeland Security Strategic Plan states. "Every terrorism lead must be pursued to its logical conclusion." The Texas Fusion Center will be an around−the−clock center that watches and warns about hazards and consolidates and analyzes information and intelligence. It is one facet of the Texas Homeland Security Strategic Plan 2005−2010 that Governor Rick Perry's office unveiled Wednesday, November 2. The proposal seeks to boost security from rural stretches along the Mexican border to refineries along the Gulf of Mexico to the way crime is monitored in major cities, Perry said. The plan focuses on building a statewide intelligence capability, enhancing multi−agency counterterrorism investigations, continually reducing vulnerabilities at critical infrastructures, ensuring public health preparedness, and expanding public awareness and involvement. It also is aimed at training first responders and ensuring that the state provides for its special needs population thoroughly before, during and after an emergency.
Source: http://www.dfw.com/mld/startelegram/news/state/13062190.htm

[Return to top]

Information Technology and Telecommunications Sector

29. *November 02, E−Commerce Times* — **Cybercrime−stopping strategies fall short according to study.** A Trend Micro study, indicates that smaller organizations, with a lack of IT support, are not able to handle security threats effectively. Requiring them to have security measures does not mean that they will actually be able to afford it. The study said that "resource−strapped organizations" with little or no IT support face a challenge in protecting themselves from malware, or attackers. said Steve Quane, general manager of Trend Micro's small and medium business operations, states "Encounters with security threats are rising faster in smaller organizations, but these same organizations are restricted by time, cost, and available resources." Within a matter of months all DMA members using e−mail for marketing are will be going to be required to use e−mail authentication systems that verify the authenticity of all e−mail messages they send. John A. Greco, Jr., president and chief executive officer of the DMA stated, "Consumers can have more confidence they are getting a legitimate, valid offer from a trusted source. Marketers get fewer false positives, increased deliverability and better protection for their brands from illegal use. It's a win−win for everybody."
Source: http://www.snpx.com/cgi−bin/news55.cgi?target=115933550?−114 34

30. *November 02, eSecurity Planet* — **Secure and productive workplace Instant Messenging.** With the possible merger of AOL’s AIM, MSN Messenger and Yahoos Messenger there will approximately 275 million users communicating over the internet. This has led to a vital part of the workday for many individuals. One of the advantages is that instant messaging allows for inexpensive communication between individuals. In addition, more recently there is now have video conferencing or voice−chats with minimal fuss and no extra charges. There are some perceived disadvantages to using IM, which includes lost productivity. However, one way to deal with this is to provide appropriate training to employees about proper usage of IM and that it should be treated much like e−mail.
Source: http://www.esecurityplanet.com/best_practices/article.php/35 61171

31. *November 02, Security Focus* — **Cisco IOS system timers heap buffer overflow vulnerability.** Cisco IOS is vulnerable to a heap based buffer overflow exploitation. Cisco has released an advisory stating that IOS upgrades are available to address the possibility of exploitation of heap based buffer overflow vulnerabilities which could lead to a Denial of Service. Security Focus was not aware if the advisory addresses a specific heap overflow or just provides security enhancements to mitigate attempts to exploit other heap overflow vulnerabilities.
Cisco Security Advisory: http://www.cisco.com/warp/public/707/cisco−sa−20051102−timers.shtml
References: http://www.securityfocus.com/bid/15275/references
Source: http://www.securityfocus.com/bid/15275/discuss

32. *November 02, Secunia* — **NetBSD update fixes multiple vulnerabilities.** There have been vulnerabilities reported in NetBSD. These vulnerabilities could be exploited by malicious, local users to gain escalated privileges, or by malicious users to cause a Denial of Service and compromise a vulnerable system, or by attacker’s attempting to bypass security restrictions and compromise a user's system. According to Seunica, the vulnerabilities have been fixed NetBSD−current (October 31, 2005) and NetBSD−1.6 branch (November 1, 2005).
Source: http://secunia.com/advisories/17389/

33. *November 02, SecuriTeam* — **Novell ZENworks patch management server SQL injection.** The Novell ZENworks Patch Management Server 6.0.0.52 is vulnerable to SQL injection in the management console. To be able to exploit this issue the administrator has to manually create a none privileged accounts as minimum to this allow exploitation. According to Secunia, there is a upgrade to ZENworks Patch Management version 6.2.2.181 on the Novell website.
Source: http://www.securiteam.com/windowsntfocus/6A0030KEKO.html

34. *November 02, French Security Incident Response Team* — **FrSIRT: Cisco airespace wireless LAN controllers unencrypted network access.** A vulnerability has been identified in Cisco Airespace Wireless LAN (WLAN) Controllers. This may be exploited by attackers to bypass security policies. This vulnerability is due to an error in the Lightweight Access Point Protocol (LWAPP) mode that accepts unencrypted traffic from end hosts even when configured to encrypt traffic, which could be exploited by attackers to send malicious traffic into a secure network.
Source: http://www.frsirt.com/english/advisories/2005/2278

35. *November 02, Security Focus* — **Simple PHP blog multiple input validation vulnerabilities.** The Simple PHP Blog is prone to multiple input validation vulnerabilities. These issues are due to a failure in the application to properly sanitize user−supplied input. An attacker may leverage these issues to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. These may facilitate the theft of cookie−based authentication credentials as well as other attacks. Security Focus did not report a solution to this vulnerability.
Source: http://www.securityfocus.com/bid/15283/discuss

36. *November 02, Government Computer News* — **DHS's inspector general audits IT systems.** An audit by the Department of Homeland Security's inspector general, Richard L. Skinner, found that many of the department's IT systems remain uncertified and unaccredited, while plans to correct weaknesses are undeveloped. The report also said contingency plans have not been developed and tested for all systems, and added that tools used to measure progress are neither complete nor current. "We recommend that DHS continue to consider its information security program a significant deficiency for [fiscal] 2005," the report concluded. DHS officials agreed with the recommendations and, according to the report, have developed remediation plans for fiscal 2006. Skinner evaluated DHS' compliance with the Federal Information Security Management Act of 2002, which focuses on program management, implementation and evaluation of the security of unclassified and national security IT systems. The department has made progress on several fronts, including developing so−called Plans of Action and Milestones, as well as a Trusted Agent FISMA tool to collect and track data related to FISMA compliance.
Report: http://www.dhs.gov/interweb/assetlibrary/OIG_05−46_Sep05.pdf
Source: http://www.gcn.com/vol1_no1/daily−updates/37474−1.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 aware of publicly available proof of concept code for an Oracle worm. Currently, US−CERT cannot confirm if this code works. We are working with Oracle to determine the threat posed by this code.

Although there is limited information concerning this potential threat, US−CERT strongly encourages Oracle system administrators to implement the following workarounds:

* Change default user credentials for Oracle installations
* Change the default port for the TNS listener
* Restrict Oracle network access to trusted hosts only
* Revoke CREATE DATABASE LINK privileges from the CONNECT role

US−CERT will continue to investigate the issue and provide updates as they become available.

For more information please review URL:
http://www.us−cert.gov/current/current_activity.html

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 4142 (oidocsvc), 135 (epmap), 80 (www), 139 (netbios−ssn), 25 (smtp), 1025 (win−rpc) 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

37. *November 03, New York Times* — **Bomb is found near congressman's office in New York.** A partly exploded pipe bomb was found in back of a building on Long Island, NY, that houses the Congressional district office of Representative Peter T. King, the Nassau County, NY, police reported Wednesday, November 2. No one was injured, the police said. It was not certain that King's office was the target, since it is one of several tenants in the building. Nor would the authorities speculate on what the motive may have been. There was no warning or claim of responsibility, King said. A Republican who was recently chosen as chairman of the House Homeland Security Committee, King said he did not know if the incident was related to his new post.
Source: http://www.nytimes.com/2005/11/03/nyregion/03bomb.html

[Return to top]

General Sector

38. *October 31, NBC 5 (TX)* — **FBI investigates cell phone purchase.** A Target store employee alerted Dallas, TX, police to a recent cellular telephone equipment purchase. A man bought $60,000 worth of prepaid cell phones. The size of the purchase raised suspicions among police investigators, who turned over the case to the FBI. The large purchase caused investigators to look toward possible homeland security threats. On two occasions during October, a man of Middle Eastern descent bought $30,000 worth of prepaid cell phones. Officials with the FBI and Target declined to comment on the case other than to say they were pleased that the clerk reported the purchase.
Source: http://www.nbc5i.com/news/5216970/detail.html?rss=dfw&psp=ne ws

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact DHS

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.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.