Department of Homeland Security Daily Open Source Infrastructure Report for 14 December 2006

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

Daily Highlights

- The Chicago Sun−Times reports that because of the theft of a company laptop computer, 382,000 Boeing Co. retirees and active workers are at risk of identity theft and credit−card fraud. (See item 6)
- The Trust for America's Health's fourth annual report, Ready or Not? Protecting the Public's Health From Disease, Disasters, and Bioterrorism, says America remains under−prepared to protect the public's health in the event of bioterrorism, bird flu, or other emergencies. (See item 25)
- The New York Times reports that in simultaneous dawn raids, Immigration and Customs Enforcement agents swept into six Swift & Company meatpacking plants, Tuesday, December 12, rounding up hundreds of immigrant workers in what was described as a vast criminal investigation of identity theft. (See item 28)

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. *December 12, U.S. Army Corps of Engineers* — **Army engineers improving electricity in Iraq.** The huge consumption of electricity as a result of the large quantity of electrical goods

the Iraqi people are buying with their increasing prosperity, combined with the sabotage of power lines, have contributed to Iraq's challenge of keeping up with electrical demands. Despite those obstacles, the U.S. Army Corps of Engineers (USACE) has made significant progress in improving electrical production and distributing power equitably throughout the country. USACE engineers oversee the building, refurbishing and upgrading of the electrical power systems, including generation, transmission and distribution countrywide according to Lt. Col. Anthony G. Reed, resident engineer for the Karbala and North Babil resident offices of the Gulf Region South District (GSR). Most projects focus on distributing electricity from one town to another, and to the outlying neighborhoods. Greg F. Fillers, GRS chief of programs and project management, said that the Corps is responsible for reporting progress on projects.
Source: http://www.grd.usace.army.mil/news/releases/NR06−12−12−2.htm l

2. *December 11, Platts Energy Bulletin* — **U.S. Congress passes bill extending tariff on ethanol imports.** The U.S. Senate Saturday, December 9, extended through January 1, 2009, a secondary tariff of 54−cents/gallon on ethanol imports into the U.S. The measure, which was part of an omnibus tax bill, passed U.S. House last Friday, and is now on its way to President Bush for his signature. The 54−cent secondary tariff on ethanol imports is designed to offset the 51−cent/gallon blender's credit that is applied to ethanol no matter its country of origin. The U.S. ethanol industry said that removing the tariff offset, which was set to expire on October 1, 2007, would have had dire consequences for the industry. American Coalition for Ethanol vice president Brian Jennings said that allowing the tariff to lapse "...would have sharply curtailed the growth of an American renewable fuels industry that has the potential for enormous benefits to the nation's economy, environment and energy security." Congress has supported growing the U.S. ethanol industry as a way to trim U.S. reliance on foreign oil. Last year, as part of the Energy Policy Act, Congress passed a renewable fuels standard requiring the use of 7.5 billion gallons of renewable fuels by 2012.
Source: http://www.platts.com/Oil/News/6330824.xml?p=Oil/News&sub=Oi l

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *December 13, Atlanta Journal−Constitution* — **Asphalt tank explodes, burns at refinery.** No one was injured early Wednesday, December 13, when a 26,000−gallon tank of molten asphalt exploded and burned in Douglas County, GA. The tank, at the Young Refining plant on Huey Road about a half−mile east of Georgia 92, blew up about 4:45 a.m. EST. The tank was about half−full and contained about 16,000 gallons of asphalt. The fire was contained to one tank, and firefighters had the flames under control by 6:15 a.m. EST. Traffic on nearby U.S. 78 was not affected by the incident. Train traffic on adjacent tracks was halted, but resumed shortly before 7 a.m. EST.
Source: http://www.ajc.com/metro/content/metro/stories/2006/12/13/12 13mettankfire.html

[Return to top]

Defense Industrial Base Sector

4. *December 12, GovExec* — **GSA, DoD reach agreement on acquisition policies.** The General Services Administration (GSA) announced Tuesday, December 12, that it has agreed to honor the Department of Defense's (DoD) interpretation of appropriations law when placing orders for DoD buyers. In an agreement signed December 4 by Shay Assad, director of defense procurement and acquisition policy, and December 6 by GSA Chief Acquisition Officer Emily Murphy, GSA officials outlined a series of steps the agency will take to placate long−standing DoD concerns about interagency contracting. The two agencies have disagreed about when federal law requires the clock to start counting the time remaining on contracts for services purchased on an annual basis, also known as "severable services" contracts. GSA's position continues to be that it has about 90 days after a fiscal year ends to obligate money from an agency to vendors. Defense says no money can be held over from one year to the next, and GSA has promised to abide by that rule for all Defense purchases made through it. The result of GSA's decision to acquiesce to DoD's interpretation will be that DoD must place its GSA orders earlier in the year than it might have previously, said David Drabkin, GSA's deputy chief acquisition officer.
   Source: http://www.govexec.com/story_page.cfm?articleid=35683&dcn=to daysnews

[Return to top]

Banking and Finance Sector

5. *December 13, Associated Press* — **SEC easing key control rules for firms.** Federal securities regulators are moving to ease some financial−control rules for thousands of smaller public companies at the same time they look to stiffen requirements for individuals to invest in fast−growing hedge funds. In proposed rule changes under a landmark 2002 anti−fraud law, the Securities and Exchange Commission (SEC) is acting in response to business complaints that a key requirement of the law enacted after the wave of corporate scandals is overly burdensome and costly. SEC Chairman Christopher Cox and the other four commissioners were tentatively adopting the revisions at a public meeting on Wednesday, December 13. The changes would especially benefit smaller companies. Smaller businesses have complained most vocally to the SEC about the costs of complying with Section 404 of the Sarbanes−Oxley law, which requires companies to file reports on the strength of their internal financial controls and to fix any problems. At the same time, addressing the rising incidence of fraud in the burgeoning hedge fund industry, the SEC is proposing to raise the minimum financial requirements for individuals wanting to invest in the high−risk pools.
   Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/12/13/AR2006121300076.html

6. *December 13, Chicago Sun−Times* — **Stolen laptop puts Boeing worker data at risk.** Because of the theft of a company laptop computer, 382,000 Boeing Co. retirees and active workers are at risk of identity theft and credit−card fraud. The files on the computer contained their names, Social Security numbers and, in most cases, also home addresses, phone numbers and birth dates as well as salary information on some. The theft, which Boeing confirmed Tuesday, December 12, is the third such incident in the past 13 months in which a laptop computer containing personnel information was stolen, and it took place despite safeguards the company put in place. As was the case in the other situations, information on the laptop wasn't encrypted. The latest theft took place in the first week of December, but Boeing has yet to

notify affected retirees and employees. They will be notified shortly either online or by mail, Boeing spokesperson Tim Neale said. The theft took place after an employee left the laptop unattended, and returned to find it gone, Neale said. Regarding the earlier thefts, he said "we haven't had any indication that anybody has misused the information."
Source: http://www.suntimes.com/business/170185,CST−FIN−boeing13.art icle

7. *December 12, Associated Press* — **Government appeals ruling that would force change in nation's currency to aid the blind.** The Bush administration on Tuesday, December 12, asked an appeals court to overturn a ruling that could require a redesign of the nation's currency to help the blind. Department of Justice (DOJ) lawyers filed the appeal with the U.S. Court of Appeals for the District of Columbia Circuit on behalf of Treasury Secretary Henry Paulson. The appeal seeks to overturn a ruling last month by U.S. District Judge James Robertson, who ordered Treasury to come up with ways for the blind to recognize the different denominations of paper currency. Robertson had ruled in a lawsuit brought by the American Council of the Blind. The council proposed several options for changes, including printing different size bills or changing the texture by adding embossed dots or foil. In the government's appeal, DOJ lawyers argued that visually impaired people are not denied "meaningful access" to money by the way the nation's currency is designed.
Source: http://abcnews.go.com/Politics/wireStory?id=2720870

8. *December 12, IDG News Service* — **'Rock Phish' blamed for surge in phishing.** While nobody knows exactly who or where they are, Rock Phish is actually a person, or perhaps a group of people, who are behind as much as one−half of the phishing attacks being carried out these days, security experts say. No one can say for sure where Rock Phish is based, or if the group operates out of a single country. Since 2004, it has grown to be one of the most prominent phishing groups in operation. It has developed a variety of new attack techniques that have earned the group a kind of grudging respect among security professionals, several of whom declined to be interviewed on the record for this story for fear of being physically harmed. They estimated that the criminal organization's phishing schemes have cost banks more than $100 million to date. Rock Phish is not known for targeting the two most popular phishing targets – eBay and PayPal. Instead, it specializes in European and U.S. financial institutions. "They are probably the most active group of phishers in the world," said Dan Hubbard, senior director, security and technology research with Websense Inc.
Source: http://www.infoworld.com/article/06/12/12/HNrockphish_1.html

9. *December 12, ZDNet (Australia)* — **Phishers target bank security upgrades.** There was a spike in phishing activity last month, with fraudsters targeting an increasing number of brands and using more sophisticated tools to try and fool online banking customers, according to the RSA Online Fraud Intelligence Report for November. According to RSA an increasing number of financial institutions have been upgrading their online banking systems in order to comply with U.S. regulations. Phishers have been using the upgrade activity to try and exploit users. Just over a year ago, five U.S. banking regulators – under the Federal Financial Institutions Examination Council's (FFIEC) umbrella – advised financial institutions to "deploy security measures to reliably authenticate their online banking customers." RSA claims that some of the most advanced phishing attacks during November tried to exploit banking customers before or during the implementation of these new systems. "The latest scam involves a phishing e−mail requesting customers to … upgrade to the bank's new security enhancement," said the RSA

report. Report: http://www.rsasecurity.com/solutions/consumer_authentication/intelreport/RSA%20Online%20Fraud%20Intel%20Report%20−%20Nov %202006.pdf
Source: http://www.zdnet.com.au/news/security/soa/Phishers_target_bank_security_upgrades_RSA/0,130061744,339272654,00.htm

[Return to top]

Transportation and Border Security Sector

10. *December 13, Associated Press* — **Talks may signal airlines' consolidation.** A flurry of confirmed and reported talks among airlines may signal merger mania within the struggling industry. UAL Corp.'s United Airlines and Continental Airlines Inc. are exploring a possible combination, according to reports. On Wednesday, December 13, AirTran Holdings Inc. said it has made a $290 million stock and cash bid for Midwest Air Group Inc. And Qantas Airways, Australia's flagship carrier, fended off a takeover bid led by an investment bank and two private−equity firms. All this activity comes on the heels of the recent hostile $8.67 billion takeover bid that US Airways Group Inc. made for Delta Air Lines Inc., whose top executive has rebuffed the offer. While airlines have rebounded from the troughs they fell into just a few years ago, mainly by laying off workers and reducing operating costs, they still must battle the high cost of fuel. Many industry analysts and consultants believe consolidation would help in this environment, by enabling carriers to cut overlapping routes and reduce available seat capacity, making it easier to raise fares.
Source: http://www.usatoday.com/travel/flights/2006−12−13−airline−co nsolidation_x.htm

11. *December 13, Washington Post* — **Rule on simulators could change how pilots are trained.** The international organization that sets the world's aviation regulations has adopted a new standard that could alter the nature of pilot training. In essence, prospective co−pilots will be able to earn most of their experience in ground−based simulators. The move is designed to allow foreign airlines, especially those in Asia and the Middle East that face shortages of pilots, to more quickly train and hire flight crews. The United States isn't expected to adopt the new rules, but international pilots trained under the new standards will be allowed to fly into and out of the country. The change is generating some controversy. Safety experts and pilot groups question whether simulators −− which have long been hailed as an important training tool −− are good enough to replace critical early flight experience. The new rules apply only to co−pilots of commercial planes. Captains, who are in charge of those aircraft, must have hundreds more hours of flight experience. The new standards will allow people to become a co−pilot on a jetliner with about 70 hours of flight time and 170 hours in simulators. Other licenses require about 200 hours of flight experience. Co−pilots perform many of the same duties as captains.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/12/12/AR2006121201384.html

12. *December 13, Gov Exec* — **IG urges CBP to better use intelligence.** Investigators recently recommended that U.S. Customs and Border Protection (CBP) strengthen its use of intelligence reports and technology for the container screening component of a system that has come under attack from privacy advocates for its use of information on travelers. A report published by the Department of Homeland Security (DHS) inspector general last week called on CBP to "fully

utilize" intelligence for the Automated Targeting System (ATS). The auditors also said port performance evaluations need improvement, and policies and procedures for inspecting high−risk shipments need tweaking. The IG examined various DHS locations in the Washington area and three "major ports of entry," checking operations, inspection results data, required training course material and programs used by CBP and other agencies that track shipments. The report urged CBP to review its policies on which port workers need security clearances, as there are currently differences in interpretation. Auditors stated that additional guidance is needed for shipments with "elevated" ATS scores for risk −− the system by which the level of inspection per container is judged. They said tracking and inspection methods for containers "need to be periodically reviewed and evaluated."
IG report: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07−09_Nov06.pdf
Source: http://www.govexec.com/story_page.cfm?articleid=35684&dcn=to daysnews

13. *December 12, Cincinnati Enquirer* — **New takeoff rules sought by NTSB.** The National Safety Transportation Board (NTSB), investigating the August 27 Comair crash that took 49 lives, says the case shows tighter procedures are needed before takeoff. Commercial aircraft crews must be given rules to confirm and cross−check their aircraft's location at the assigned departure runway before getting into position for takeoff, the NTSB said on Tuesday, December 12. The agency also said commercial airlines need to establish specific guidelines on runway lighting requirements for nighttime takeoffs. Doomed Comair Flight 5191 crashed August 27 after pilots attempted an early morning takeoff from the wrong runway, also unlit, at Lexington's Blue Grass Airport. The runway, which was half as long as the one the jet should have used, was too short for the Bombardier CRJ−200 to safety get airborne. The NTSB said its investigation revealed that Comair did not provide guidance to its pilots about conducting takeoffs at night on unlighted runways. Comair spokesperson Kate Marx said the airline complies with all federal rules and guidelines, but will continue to review its policies and procedures in light of the NTSB's report.
NTSB Recommendation A06_83_84: http://www.ntsb.gov/recs/letters/2006/
Source: http://news.enquirer.com/apps/pbcs.dll/article?AID=/20061212 /BIZ01/312120037/−1/all

14. *December 12, USA TODAY* — **Giant jet sets off fuel tank concerns.** Federal accident investigators and safety advocates say they are worried that the Airbus A380 double−decker jet will be exempt from new U.S. rules designed to prevent fuel tank explosions like the one that downed TWA Flight 800 in 1996. European officials have said that they do not agree with fuel tank safety rules proposed in the United States and will not make the mammoth new plane subject to them. U.S. and European regulators on Tuesday, December 12, gave Airbus approval to fly passengers on the largest jetliner in history, but left unresolved the fuel tank issues. The U.S. Federal Aviation Administration says it intends to release a final fuel tank rule next year. As proposed, the rule would only apply to U.S.−registered aircraft. If Europeans do not adopt the rule, foreign carriers would be free to fly A380s into this country without updating the jet's fuel tanks. The National Transportation Safety Board (NTSB) declined comment, but the agency took the unusual step of writing to European regulators in 2004 to urge fuel tank safety measures on the A380. The NTSB said that without the measures, the jumbo jet could be vulnerable to an explosion.
NTSB 2004 letter to European regulators:
http://www.usatoday.com/news/washington/ntsb_scan.pdf

Source: http://www.usatoday.com/travel/flights/2006−12−12−airbus−saf ety_x.htm

15. *December 06, NTSB News* — **NTSB urges airlines to change runway−stopping calculations.** National Transportation Safety Board (NTSB) Chairman Mark V. Rosenker is urging airlines to voluntarily adopt changes in the way they calculate stopping distances on contaminated runways, in accordance with Federal Aviation Administration (FAA) guidance issued in response to an urgent NTSB recommendation. On December 8, 2005, Southwest Airlines flight 1248, a Boeing 737−7H4, landed on runway 31C at Chicago Midway Airport during a snowstorm. The aircraft failed to stop and came to rest on a roadway after striking two vehicles and killing a six−year−old boy. While approaching Chicago on a flight from Baltimore, the pilots used an on−board laptop performance computer (OPC) to calculate expected landing performance. Information entered into the computer included expected landing runway, wind speed, and direction, airplane gross weight at touchdown, and reported runway braking action. The OPC then calculated the stopping margin. If the thrust reverser credit had not been allowed in calculating the stopping distance for flight 1248, the OPC would have indicated that a safe landing on runway 31C was not possible. The FAA subsequently announced that it believes it needs to propose this change through the rulemaking process, which will delay implementation of this change.
A copy of the recommendation letter may be found on the Board's Website:
http://www.ntsb.gov/Recs/letters/2006/A06_16.pdf
Source: http://www.ntsb.gov/Pressrel/2006/061206.htm

16. *November 13, Government Accountability Office* — **GAO−07−15: Intercity Passenger Rail: National Policy and Strategies Needed to Maximize Public Benefits from Federal Expenditures (Report).** Intercity passenger rail service is at a critical juncture in the United States. Amtrak, the current service provider, requires $1 billion a year in federal subsidies to stay financially viable but cannot keep pace with its deteriorating infrastructure. At the same time, the federal government faces growing fiscal challenges. To assist the Congress, the Government Accountability Office (GAO) reviewed (1) the existing U.S. system and its potential benefits, (2) how foreign countries have handled passenger rail reform and how well the United States is positioned to consider reform, (3) challenges inherent in attempting reform efforts, and (4) potential options for the federal role in intercity passenger rail. GAO analyzed data on intercity passenger rail performance and studied reform efforts in Canada, France, Germany, Japan, and the United Kingdom. GAO recommends that Congress consider restructuring the nation’s intercity passenger rail system. Any change should include establishing clear goals for the system, defining the roles of key stakeholders, and developing funding mechanisms that include cost sharing between the federal government and other beneficiaries. Amtrak agreed intercity passenger rail is at a critical juncture and said that reform includes establishing national policy goals, stakeholder roles, and committed funding.
Highlights: http://www.gao.gov/highlights/d0715high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−15

17. *November 13, Government Accountability Office* — **GAO−07−25: Next Generation Air Transportation System: Progress and Challenges Associated with the Transformation of the National Airspace System (Report).** In 2003, Congress created the Joint Planning and Development Office (JPDO) to plan for and coordinate, with federal and nonfederal stakeholders, a transformation from the current air traffic control system to the “next generation

air transportation system" (NGATS) by 2025. Housed within the Federal Aviation Administration (FAA), JPDO has seven partner agencies: the Departments of Transportation, Commerce, Defense, and Homeland Security; FAA; the National Aeronautics and Space Administration (NASA); and the White House Office of Science and Technology Policy. FAA will have primary responsibility for implementing NGATS. This report addresses (1) the status of JPDO's efforts to plan for NGATS, (2) the key challenges facing JPDO, and (3) the key challenges facing FAA as it implements the transformation. To address these issues, the Government Accountability Office (GAO) reviewed relevant documents, interviewed agency officials and stakeholders, and conducted an expert panel. GAO recommends that JPDO institutionalize its practices for interagency collaboration and assess stakeholder involvement, and that FAA assess its needs for technical expertise. JPDO and FAA commented that they plan to consider GAO's recommendations. NASA highlighted the impact of its refocused aeronautics research. GAO incorporated the other agencies' technical comments as appropriate.
Highlights: http://www.gao.gov/highlights/d0725high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−25

[Return to top]

Postal and Shipping Sector

18. *December 11, KRT Wire* — **Link sought between hoax letters and ricin.** Federal investigators are looking into a possible link between recent hoax letters, each containing a white powder and believed to have been sent by a Texas prison inmate, to determine whether they are related to a small shipment of the poison ricin to a mailing center in South Carolina in 2003. Someone calling himself the Fallen Angel signed at least one of the six recent letters −− sent to government officials in Washington, Baltimore and Buffalo, NY −− and the ricin letter, which was received at a mail−processing facility in Greenville, SC, in October 2003, an FBI alert said. The high priority alert, dated late last month, said the U.S. Clerk's Office in Buffalo on November 20 received one of the letters, which was signed "Fallen Angel" and contained a nontoxic powder. The letter "included references to anthrax and threats to the President," and its sender is believed to be an inmate who is serving life in prison for "use of weapons of mass destruction," the alert said. The prisoner, who was not identified, is at the Montford state prison unit in Lubbock, TX, and will be transferred to a federal prison, the alert said.
Source: http://www.mercurynews.com/mld/mercurynews/news/politics/162 17030.htm

[Return to top]

Agriculture Sector

19. *December 13, World Organization for Animal Health* — **OIE mandates support Biological and Toxin Weapon Convention's crucial objectives.** Eighty percent of pathogenic agents that can potentially be used in bioterrorism are zoonotic −− that is, animal pathogens with the capacity to infect humans. "The OIE is committed to take an active part in counteracting bioterrorism as its work falls within the objectives of the Biological and Toxin Weapon Convention in the field of prevention and control of animal diseases events whether deliberate or natural," said Dr. Gideon Brückner, Head of the World Organization for Animal Health

(OIE) Scientific and Technical Department. Thwarting bioterrorism threats linked with animal pathogens goes through the improvement of national veterinary services governance. The weaker the veterinary services of a country, the more prone it is to acts of bioterrorism. The OIE developed and launched the World Animal Health Information System. Through this Web−based application, animal health information is disseminated immediately to member countries and made readily available to the general public. Also, the OIE, in collaboration with the World Health Organization and the United Nations Food and Agriculture Organization developed a Global Early Warning and Rapid Response system which allows linking the human and animal pathogen interface through the sharing of complimentary information on zoonotic diseases and animal diseases.
Source: http://www.oie.int/fr/press/fr_061213_BTWC.htm

20. *December 12, Agricultural Research Service* — **Weed implicated in potato blight persistence.** Late blight, the devastating tuber disease that triggered the Irish potato famine of the mid−1800s, has a new partner in crime. Scientists with the Agricultural Research Service (ARS) discovered that Phytophthora infestans −− the microorganism behind the blight −− is seeking refuge in potato fields, holed up in an alternate host plant: hairy nightshade. As extension agents in the northern part of the Maine discovered, hairy nightshade plants were showing up speckled with suspicious dark and oily spots. Researchers analyzed the microorganisms on the plants and verified, for the first time, that hairy nightshade is an alternate host of P. infestans in Maine. To make matters worse, a limited survey found that 55 percent of fields assessed in the state contained the plant.
Source: http://www.ars.usda.gov/is/pr/2006/061212.htm

21. *December 12, Cattle Network* — **Kansas State teams with agencies to fight Johne's disease in cattle.** Kansas cattle producers eager to prevent Johne´s disease in their herds now have some help, thanks to the Kansas Voluntary Johne´s Disease Control programs for dairy and beef cattle. "Johne´s disease is a chronic and incurable intestinal infection of cattle and other ruminant animals," said Larry Hollis, veterinarian with Kansas State Research and Extension. Once sufficient damage to the intestinal lining occurs, the disease causes chronic diarrhea and rapid weight loss. There is no effective treatment for the disease, he said. The benefits of testing cattle herds voluntarily are numerous, Hollis said. Producers with infected herds incur losses from premature culling, reduced milk production, lower fertility and increased heifer replacement costs. Poor body condition also lowers cull cow sale prices. Herds with negative tests may receive premiums as demand for Johne´s disease−free animals increases, he added.
Source: http://www.cattlenetwork.com/content.asp?contentid=90533

22. *November 15, Government Accountability Office* — **GAO−07−35: USDA Conservation Programs: Stakeholder Views on Participation and Coordination to Benefit Threatened and Endangered Species and Their Habitats (Report).** Authorization for several conservation programs administered by the U.S. Department of Agriculture (USDA) expires in 2007, raising questions about how these programs may be modified, including how they can better support conservation of threatened and endangered species. Private landowners receive funding under these programs to implement conservation projects directed at several resource concerns, including threatened and endangered species. In this report, the Government Accountability Office (GAO) discusses (1) stakeholder views on the incentives and disincentives to participating in USDA programs for the benefit of threatened and endangered

species and their suggestions for addressing identified disincentives and (2) coordination efforts by USDA and the U.S. Fish and Wildlife Service (FWS) to benefit threatened and endangered species. In performing this work, GAO conducted telephone surveys with a nonprobability sample of over 150 federal and nonfederal officials and landowners. GAO recommends that USDA and FWS include mechanisms for monitoring and reporting on coordination efforts in the final version of the agencies' memorandum of understanding. USDA and the Department of the Interior commented that they generally concurred with the findings and recommendations.
Highlights: http://www.gao.gov/highlights/d0735high.pdf
Source: http://www.gao.gov/cgi-bin/getrpt?GAO-07-35

[Return to top]

Food Sector

23. *December 12, WHBF-TV (IL)* — **E. coli outbreaks in Iowa and Minnesota.** More people in the Midwest have been infected with E. coli. Minnesota health officials say seven cases have been confirmed in the state. Interviews with the patients have revealed they all ate at Taco John's restaurant between November 30th and December 2nd. Meanwhile, in Cedar Falls, IA, 40 people who also ate at a Taco John's have been sick in a suspected E. coli outbreak. Health officials say there's no evidence to suggest the outbreaks in Minnesota and Iowa are connected, but they're not ruling it out.
Source: http://www.whbf.com/Global/story.asp?S=5806239&nav=0zGo

[Return to top]

Water Sector

24. *December 12, Reuters* — **Satellites detect major decreases in Africa water.** A pair of orbiting satellites have surveyed the Earth's water in unprecedented detail, showing sharp decreases in parts of Africa over the past five years, scientists said on Tuesday, December 12. "This is the first time we have been able to track these variations," Jay Famiglietti, an Earth system sciences professor at the University of California, Irvine, told the fall meeting of the American Geophysical Union. By detecting the gravitation pull of water, the Gravity Recovery and Climate Experiment, or GRACE, launched in 2002, measures water both above and below the Earth's surface, amounts that are in constant flux. The nearly five-year-old partnership between NASA and the German Aerospace Center has found that over a three-year period water storage along the Congo River Basin has decreased by nearly double the amount Africans consume annually, excluding irrigation, Famiglietti said. The GRACE data also found drying along the Zambezi and Nile basins in Africa, and increases along the American Mississippi and Colorado River basins. "We know that things go up and down so there is no cause for alarm," Famiglietti said, adding that scientists need a longer period of data to make more definitive conclusions.
Source: http://www.alertnet.org/thenews/newsdesk/N12358263.htm

[Return to top]

Public Health Sector

25. *December 12, HealthDay* — **U.S. underprepared to protect public health: Report.** Five years after the September 11 terrorist attacks, America is still woefully under−prepared to protect the public's health in the event of bioterrorism, bird flu or other emergencies. That's the assessment of Trust for America's Health's fourth annual report, Ready or Not? Protecting the Public's Health From Disease, Disasters, and Bioterrorism, released Tuesday, December 12. Among the report's other major findings: a) Only 15 states were rated at the highest preparedness level in terms of their ability to provide emergency vaccines, antidotes and medical supplies from the Strategic National Stockpile; b) Half the states would run out of hospital beds within two weeks of a moderate flu pandemic and 47 states would run out of beds within two weeks of a severe flu pandemic; c) Forty states currently have a shortage of registered nurses, let alone what would be needed in a crisis; d) Eleven states plus the District of Columbia lack the capability to test for biological threats in laboratories.
Report: http://healthyamericans.org/reports/bioterror06/BioTerrorRep ort2006.pdf
Source: http://health.yahoo.com/news/169858;_ylt=At.cxsG313ouOcrW57L isx0qLcsF

26. *December 12, Seattle Post−Intelligencer* — **Adult measles case confirmed in Seattle.** Public health officials in Seattle and King County have confirmed a case of imported measles. An adult traveler who acquired the potentially severe infectious disease, also known as rubeola, did visit a small number of public places while contagious. The person with measles returned December 8 to Seattle on Alaska Airlines Flight 399 and sought medical attention immediately. Authorities with Public Health are working to identify those who might have been exposed at the health facility. Other possible exposures could have occurred December 8 in the lobby of the Warwick Seattle Hotel, 401 Lenora St.
Source: http://seattlepi.nwsource.com/local/295610_measles12ww.html

27. *December 12, Associated Press* — **Seniors quarantined after norovirus outbreak in three California nursing homes.** Elderly residents at three San Mateo County, CA, nursing homes were told to avoid common areas and eat meals in their rooms after an outbreak of the highly contagious norovirus, health officials said Tuesday, December 12. The quarantine was imposed as a precaution after 85 people at the Bonnie Brae Terrace facility in Belmont and 21 residents of two other homes became ill or showed flu−like symptoms of the gastrointestinal bug. Tests to confirm it was norovirus that sickened people at the two homes. A similar outbreak also was reported Monday at the county hospital, where 12 patients in the long−term care unit and 13 employees suffered from the vomiting, diarrhea, and fever associated with norovirus.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/states /california/northern_california/16224298.htm

[Return to top]

Government Sector

28. *December 13, New York Times* — **ICE agents raid meat plants in identity theft case.** In simultaneous dawn raids, federal immigration agents swept into six Swift & Company meatpacking plants in six states, Tuesday, December 12, rounding up hundreds of immigrant

workers in what the agents described as a vast criminal investigation of identity theft. More than 1,000 agents from Immigration and Customs Enforcement (ICE) appeared at 6:00 a.m. at the Swift plants with warrants to search for illegal immigrants. In a new enforcement tactic, federal officials said they planned to bring criminal charges against some of the immigrants accused of using stolen identities. They said the raids were tied to complaints from United States citizens who discovered that their names were being used by Swift plant workers. “There are several hundred Americans who were victimized,” said Marc Raimondi, an ICE spokesperson. ICE officials said the operation focused on immigrants who had obtained documents with identity information corresponding to that of United States citizens, in some cases by buying them from underground organizations that traffic in false documents. The immigration agency raided plants in Hyrum, UT; Greeley, CO; Cactus, TX; Grand Island, NB.; Marshalltown, IA; and Worthington, MN.
Source: http://www.nytimes.com/2006/12/13/us/13raid.html

[Return to top]

Emergency Services Sector

29. *December 12, Federal Computer Week* — **Northcom's new C2: collaboration and communications.** The U.S. Northern Command (Northcom) has adopted the phrase collaboration and communication instead of classic military command and control (C2), said Admiral Timothy Keating, Northcom commander. The command, headquartered in Colorado Springs, CO, must dovetail its operations with 60 other federal agencies or departments to help coordinate the Department of Defense’s response to disasters or an attack on the United States. When Northcom responds to a disaster, Keating said, he’s less concerned with C2 and more concerned about collaboration and coordination with civil agencies that can provide a “unity of results that comes from a unity of effort.” Bernd McConnell, Northcom’s director of Interagency Coordination, said to facilitate interagency cooperation, representatives from about 60 agencies, including the Department of Homeland Security and the Federal Emergency Management Agency, work at Northcom. His group works to facilitate communication among those agencies and to ensure there is a unified response to a disaster at a local level.
Source: http://fcw.com/article97086−12−12−06−Web

30. *December 12, Federal Emergency Management Agency* — **President declares major disaster for New York.** The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Tuesday, December 12, that federal disaster aid has been made available for New York to supplement state and local recovery efforts in the area struck by severe storms and flooding during the period of November 16−17. FEMA Director David Paulison said federal funding is available to state and eligible local governments and certain private nonprofit organizations on a cost−sharing basis for emergency work and the repair or replacement of facilities damaged by the severe storms and flooding in the counties of Broome, Chenango, Delaware, Hamilton, Herkimer, Montgomery, Otsego, and Tioga.
Source: http://www.fema.gov/news/newsrelease.fema?id=32109

31. *December 12, Federal Emergency Management Agency* — **President declares major disaster for Washington.** The head of the U.S. Department of Homeland Security’s Federal Emergency Management Agency (FEMA) announced Tuesday, December 12, that federal disaster aid has

been made available for the state of Washington to supplement state and local recovery efforts in the area struck by severe storms, flooding, landslides, and mudslides during the period of November 2−11. FEMA Director David Paulison said the assistance was authorized under a major disaster declaration issued for the state by President Bush. The President's action makes federal funding available to affected individuals in the counties of Clark, Cowlitz, Grays Harbor, King, Lewis, Pierce, Skagit, Skamania, Snohomish, Thurston, and Wahkiakum.
Source: http://www.fema.gov/news/newsrelease.fema?id=32111

[Return to top]

Information Technology and Telecommunications Sector

32. *December 13, IDG News Service* — **Expert warns on wireless security in Asia.** The fast growth in wireless Internet use throughout Asia leaves users vulnerable to data theft over unsecured networks and lost or stolen mobile devices, a security expert warned Tuesday, December 12. Citrix Systems Inc. Chief Security Officer Kurt Roemer said during an interview that trends in Asia suggest increasing vulnerability as time goes on because wireless use is growing much faster than fixed−line use in many countries. Japan, for example, is a global leader in developing 3G (third−generation) mobile networks and applications, which is increasing demand for smarter phones that can handle more data and computing work −− the kind that increases the likelihood of stolen data. And in developing countries such as China and India, there are more wireless networks going up than fixed−line networks, a danger because fixed−line networks are easier to secure. Mobile devices themselves are also cause for security concern. Hard drive memory space is growing so fast that users can keep an awful lot of sensitive information on one device, he said.
Source: http://www.infoworld.com/article/06/12/13/HNasiawirelesssecu rity_1.html

33. *December 13, VNUNet* — **Firms still struggling with compliance regulations.** Compliance management is still largely a manual process which forces many IT organizations to devote "major staff resources" to reporting, new research has revealed. Among organizations with more than 5,000 employees, 80 percent require four or more full−time employees to manage data compliance, with 24 percent needing more than 10, according to a new Oracle Applications Users Group survey. The report found that, despite years of effort and millions of dollars of investment, nearly 61 percent of companies have not yet completed implementation of their Sarbanes−Oxley (SOX) compliance processes. At the same time, about 64 percent of those tracking SOX metrics have already identified deficiencies within their financial/ERP database environments related to SOX. The survey is based on the responses of more than 200 enterprise IT managers and professionals.
Source: http://www.vnunet.com/vnunet/news/2170894/firms−struggling−c ompliance

34. *December 13, CNET News* — **Symantec files piracy lawsuit.** Symantec announced Wednesday, December 13, it filed a copyright infringement lawsuit against a network of eight businesses and seven individuals, alleging they reaped an estimated $15 million in profits from pirated copies of Symantec's most popular security software. The lawsuit, filed in a U.S. District Court in Los Angeles, comes after an investigation of more than two years, the company says. The lawsuit names ANYI, SILI, GT Micro, ASP Solutions, Mark Ma, Mike Lee, John Zhang and other affiliates as defendants. "ANYI, SILI and their affiliates run a global

counterfeit distribution operation with a major focus in the United States and Canada," William Plante, Symantec's senior director of corporate security and brand protection, said in a statement. Symantec alleges the parties engaged in trademark infringement, copyright infringement, fraud, unfair competition and false advertising.
Source: http://news.com.com/Symantec+files+piracy+lawsuit/2100−7348_3−6143352.html?tag=nefd.top

35. *December 12, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−346A: Microsoft updates for multiple vulnerabilities.** Microsoft has released updates to address vulnerabilities in Microsoft Windows, Visual Studio, Microsoft Outlook Express, Microsoft Media Player, and Microsoft Internet Explorer as part of the Microsoft Security Bulletin Summary for December 2006. The most severe vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial−of−service on a vulnerable system. Note that in addition to the regular monthly security bulletins, Microsoft has also published updates for the Apple Mac versions of Microsoft Office.
Systems affected: Microsoft Windows; Microsoft Visual Studio; Microsoft Outlook Express; Microsoft Media Player; Microsoft Internet Explorer; Microsoft Office 2004 for Mac; Microsoft Office v. X for Mac.
Further information is available in the US−CERT Vulnerability Notes Database: http://www.kb.cert.org/vuls/byid?searchview&query=ms06−dec
Solution: Microsoft has provided updates for these vulnerabilities in the December 2006 Security Bulletins. The Security Bulletins describe any known issues related to the updates. Note any known issues described in the Bulletins and test for any potentially adverse affects in your environment. System administrators may wish to consider using an automated patch distribution system such as Windows Server Update Services.
Microsoft Security Bulletin: http://www.microsoft.com/technet/security/bulletin/ms06−dec.mspx
Source: http://www.uscert.gov/cas/techalerts/TA06−346A.html

36. *December 12, VNUNet* — **QuickTime flaw could go beyond MySpace.** The QuickTime security hole that enabled a phishing worm to attack users of social networking site MySpace is leaving more users and Websites vulnerable than was first thought. Security firm F−Secure said that the vulnerability has been confirmed to exist in Mac versions of QuickTime, as well as the QuickTime Alternative codec package. Apple, which makes and distributes QuickTime, distributed the fix to MySpace which then offered the patch to users who accessed the site with Internet Explorer and a detectible version of QuickTime. But this move leaves millions of users unprotected, according to F−Secure. Other browsers, including Firefox and Safari, remain exposed, and all sites that allow users to upload QuickTime movies will be vulnerable to the same sort of worm that plagued MySpace. The worm spreads itself through the profile pages of MySpace users, altering the profiles of anyone who views the infected page and redirecting them to a MySpace phishing site. This malicious site then uses stolen passwords to propagate spam messages with links to adware−installing sites.
Source: http://www.vnunet.com/vnunet/news/2170725/quicktime−bug−beyo nd−myspace

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	6699 (napster), 44113 (−−−), 1026 (win−rpc), 4207 (vrml−multi−use), 4662 (eDonkey2000), 1027 (icq), 1028 (−−−), 4672 (eMule), 6881 (bittorrent), 31621 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS 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

material.