



Department of Homeland Security Daily Open Source Infrastructure Report for 02 May 2007

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- A new video on YouTube shows the discovery of individuals' social security numbers, bank account balances and numbers, and other sensitive information in trash bags outside JPMorgan Chase Bank branches in New York City. (See item [11](#))
- The San Francisco Chronicle reports the day after a fiery gasoline truck accident destroyed key ramps in the MacArthur Maze interchange, security analysts and truck drivers weighed the scope of damage a deliberate terrorist attack using tankers could cause U.S. metropolises and highways. (See item [13](#))
- The Department of Agriculture and the Food and Drug Administration have learned that byproducts from pet food manufactured with contaminated wheat gluten imported from China have been used in chicken feed on some farms in the state of Indiana. (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. *April 30, Reuters* — **BP cost cuts may have caused big Alaska oil spill.** A powerful congressional committee said on Monday, April 30, it had evidence that deep cost cuts at oil major BP may have been a major factor behind pipeline corrosion that caused the largest ever

onshore oil spill in Alaska last year. Government-ordered inspections turned up further severe corrosion in another transit pipeline, forcing the partial closure of Prudhoe Bay, the largest oil field in the United States, for several months. BP officials rejected accusations that its cost cutting program led to unsafe operations at congressional hearings last year and outgoing BP chief executive John Browne characterized the Alaska corrosion management program as "world class." However, BP e-mails and other documents "suggest that budget pressures were severe enough that some BP field managers were considering... reducing corrosion inhibitor to save money," wrote Representative John Dingell (D), chairman of the House Energy and Commerce Committee, in a letter sent to BP on Monday. A Department of Transportation (DOT) investigation into the spills continues to focus on BP's maintenance practices. BP is currently replacing all 16 miles of transit pipelines at Prudhoe Bay and said it is reviewing its corrosion management practices.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/30/AR2007043000734.html>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

2. *May 01, WFSB (CT)* — **Tractor-trailer spills diesel on I-95.** A disabled tractor-trailer that has leaked diesel fuel closed northbound Interstate 95 on Tuesday morning, May 1, in East Haven, CT. The highway was closed until about 10 a.m. EDT near Exit 50 and delayed traffic on southbound Interstate 91 where it meets with I-95. Traffic was tied up for nearly three hours as hazardous materials crews tried to sop up the fuel. State police said nearly 100 gallons of fuel leaked from the tractor-trailer.

Source: <http://www.wfsb.com/news/13229640/detail.html>

3. *May 01, Click2Houston* — **Chemical plant catches fire.** A Brazoria County, TX, chemical plant reopened after a fire early Tuesday, May 1. Officials with the Stratton Ridge Dow Chemical Company plant in F.M. 523 near County Road 226 said the fire started in a pump. The company used a siren to alert the community to a fire but a shelter-in-place was not ordered. Residents were told not to drive down the road leading to the plant.

Source: <http://www.msnbc.msn.com/id/18413989/>

4. *April 29, WBNS-10TV (OH)* — **Hazmat situation ends safely.** A Hazmat situation that caused evacuations in a trailer park in Grove City, OH, is over, and the some 400 people evacuated are back in their homes. It was around 9 p.m. EDT Sunday night, April 29, when at least 250 trailers in a park on Georgesville Road were evacuated because of an apparent ammonium nitrate leak at a nearby farm. During that evacuation some residents were taken to a nearby elementary school, while others waited at a local gas station.

Source: <http://www.10tv.com/?sec=news&story=sites/10tv/content/pool/200704/960043470.html>

[\[Return to top\]](#)

Defense Industrial Base Sector

5. *April 30, Federal Times* — **Contractor faces possible suspension for alleged overbilling, poor performance on Iraq reconstruction work.** The Army is considering debarring Parsons Corp., one of the largest contractors in Iraq, because of allegations the company double billed the government and delivered shoddy work on a number of Iraqi reconstruction contracts. Army procurement fraud officials formally asked Parsons last month to explain why it should not be considered for debarment in the wake of a damning report by the Special Inspector General for Iraqi Reconstruction (SIGIR), which found the company failed to properly oversee subcontractors and lacked project controls and standards of conduct. In its latest quarterly report released Monday, April 30, the SIGIR reported the company double-billed the Army \$77 million for work it performed on Iraq construction projects.
SIGIR Report: <http://www.sigir.mil/reports/quarterlyreports/Apr07/Default.aspx>
Source: <http://federaltimes.com/index.php?S=2723649>

[[Return to top](#)]

Banking and Finance Sector

6. *May 01, Sophos* — **Electronic postcard arrives with a Web sting in its tail.** Sophos has warned computer users to be wary of unsolicited e-mails and defend their Web gateways, following a spam campaign that poses as an electronic postcard, but is really an attempt to lure the unwary into being infected by a Web-based Trojan horse. E-mails seen by experts at SophosLabs have the subject line "You have received a postcard!". Users who follow the Web link are taken to a downloadable executable file (postcard.exe). The file is designed to allow remote hackers to gain access to the infected Windows computer.
Source: http://www.sophos.com/pressoffice/news/articles/2007/05/post_card.html
7. *April 30, The Weekly (GA)* — **Georgia Office of Consumer Affairs dismantles organized ID fraud ring.** Criminal investigators from the Georgia Governor's Office of Consumer Affairs (OCA) and special agents from the United States Secret Service (USSS), and others, have shut down a major fake ID and counterfeit check manufacturer and made several key arrests in an identity fraud ring that operated up and down the East Coast from Florida to New Jersey for several years. Starting with data breaches at an Atlanta-based health care facility and a well-known check-processing company, investigators traced the crime to the top, where they uncovered an underground facility that manufactured counterfeit checks and fake IDs, including driver's licenses, student ID cards and fraudulent employee identification cards, which were used by the group and supplied to other fraud rings. On a single computer confiscated in the seizure investigators discovered over 2,400 Photoshop files of completed fake IDs, among which were driver's licenses from Georgia, North Carolina, Tennessee, Maryland, Alabama, Kansas, Mississippi, California and many other states. Other equipment seized included cameras, identification card printers and professional grade check printers. This is the third counterfeit ID manufacturing scheme that OCA and USSS have exposed in the seven-week period beginning March 7, 2007.
Source: http://www.theweekly.com/news/2007/April/30/fraud_ring.html
8. *April 30, Associated Press* — **Debate revived over private use of terror watch lists.** The Lawyers Committee for Civil Rights of the San Francisco Bay Area alleges that more

Americans than ever are being mistakenly connected to the Treasury Department's Office of Foreign Assets Control (OFAC) list of persons and companies engaging in or affiliated with terrorism. The report, titled "How a Treasury Department Terrorist Watchlist Ensnares Everyday Customers," concludes that "a growing number of Americans have endured stigma and lost opportunities in ordinary consumer settings" like buying a car or home. OFAC spokesperson Molly Millerwise said: "We have seen success, being able to choke off terror financing and proliferation financing...It's hard to set markers. Your success is the attack that didn't happen. But it's making it harder for terrorists to make, move and store money." The Terrorist Assets Report reports that as of 2005, the government has blocked \$13.7 million in terror funds specifically through persons and entities listed on the Specially Designated Nationals and Blocked Persons list. In 2005, the U.S was blocking \$479 million in funds connected to six countries listed as state sponsors of terrorism.

Report: How a Treasury Department Terrorist Watchlist Ensnares Everyday Customers:

<http://www.lccr.com/03%202007%20OFAC%20Report.pdf>

Source: <http://www.foxnews.com/story/0,2933,269305,00.html>

9. *April 30, Bank Net 360* — **Phishing scams being defeated faster.** Security researchers are getting better at limiting the damage caused by phishing. An example is the work of the Phishing Incident Reporting and Termination Squad (PIRT). PIRT is dedicated to taking down phishing Websites. The 15 PIRT security research volunteers have honed the time it takes to dismantle a phishing site to as little as 11 minutes. The average time, however, is a couple of hours, because of the volume of received phishing notices, said Robin Laudanski, PIRT team leader. By developing working relationships with global Internet service providers, as well as law enforcement, PIRT team members can orchestrate take-downs of phishing Websites hosted by both U.S.-based and international ISPs. Laudanski says dealing with overseas ISPs is not any harder than dealing with domestic ones, because of the established relationships. PIRT also stores and distributes the information it collects to law enforcement, financial institutions, and other corporations that request it. Banks and credit unions are the No.1 target for phishers. Recently, MIRT — Malware Incident Reporting and Termination, and SIRT — Spam Incident Reporting and Termination were launched to combat malware and spam in the same fashion. Source: http://www.banknet360.com/news/NewsAbstract.do?na_id=8689&service_id=1&bi_id=

10. *April 30, Reuters* — **Major brands see rise in online fraud.** Corporate brands face multipronged assaults from fraudulent online attackers, according to a report published Monday, April 30, that quantifies the scope of the most common threats. MarkMonitor said its new "Brandjacking Index" found cybersquatting — in which illicit sites usurp popular trademarks — false association, phishing and click fraud as major threats. A survey of public Websites recently completed found cybersquatting posed the greatest threat to brands. Phishing and domain "kiting"—the rapid registering and dropping of similar-sounding Website names — are on the rise. The study tracked daily mentions on 134 million public Web records for the world's top 25 brands, along with major brands from eight industrial categories such as autos, apparel, and high tech. Click fraud was identified 50,743 times, while e-commerce fraud occurred 21,093 times and kiting 11,015. Banks and other financial services are the mostly likely victims of kiting and phishing. The number of phishing attacks grew 104 percent during March from the same month in 2006, with more than 229 brand name companies, mostly financial services firms, coming under assault. The latest quarter was the first time banks had

outpaced online auctions such as eBay as targets. Auctions suffered 36 percent of phishing attacks.

Source: http://news.com.com/Major+brands+see+rise+in+online+fraud/2100-7355_3-6180176.html?tag=cd.top

- 11. *April 30, KSFY (NY)* — YouTube video shows customer names and account numbers.** A new video on YouTube shows the discovery of individuals' social security numbers, bank account balances and numbers, and other sensitive information in trash bags outside JPMorgan Chase Bank branches in New York City. The personal and financial information found on the street in Chinatown, Queens, the Upper East Side, and in two Brooklyn locations could be used to perpetrate identity theft. Identity theft concerns and other issues around JPMorgan Chase are the topic of a new blog, www.chastrash.org. According to the Department of Justice, criminals who engage in "dumpster diving" can sometimes cobble together enough personal identifying information to steal someone's identity and make fraudulent withdrawals from bank accounts, and apply for loans and credit cards. New York State has the nation's highest rate of identity theft according to research release by ID Analytics Inc. in February 2007.

Source: <http://www.ksfy.com/news/business/7257171.html>

[[Return to top](#)]

Transportation and Border Security Sector

- 12. *May 01, Associated Press* — Air traffic controllers: FAA radio ban threatens safety.** An eight month–old Federal Aviation Administration (FAA) ban on radios in air traffic control towers could put lives at risk when severe weather bears down on airports, a national labor union says. At issue is a contract with the National Air Traffic Controllers Association implemented in September by the FAA that removed AM/FM radios from tower work areas to prevent them from becoming a distraction to controllers. But taking the radios means controllers lose a key asset they use to monitor the funnel clouds of a tornado and relay that information to pilots in the air, the air traffic controllers association says. The FAA said the controllers already have a "large amount of weather information" in the tower. Controllers receive information about precipitation and wind patterns from equipment available in the tower, but cannot hear tornado alerts the National Weather Service is putting out to the public, according to the union. The FAA allows radios and TVs in the break rooms, but those are often out of earshot to controllers, the union says. Since the ban, the union says there have been at least a half–dozen near miss "tornado vs. tower events," including Oklahoma City, Tulsa and Denver.

Source: http://www.usatoday.com/travel/news/2007-04-30-faa-radio-ban_N.htm

- 13. *May 01, San Francisco Chronicle* — Freeway collapse shows cities vulnerable if tankers used as weapons.** The day after a fiery gasoline truck accident destroyed key ramps in the MacArthur Maze interchange, security analysts and truck drivers weighed the scope of damage a deliberate terrorist attack using tankers could cause U.S. metropolises and highways. Security experts said the crash — and the costly repairs — demonstrated how easy it would be for terrorists to disrupt normal life in major U.S. cities. San Francisco Mayor Gavin Newsom has called the accident a giant wake–up call, saying it highlighted how vulnerable San Francisco is to a potential terrorist attack. Truck drivers already are required to undergo a mandatory

background check to haul hazardous materials, such as gasoline, said Nico Melendes, spokesperson for the Transportation Security Agency. But background checks do not prevent gasoline tankers from being stolen or hijacked by determined terrorists, said John Conley, president of National Tank Truck Carriers, Inc., an association of truckers. More than 800,000 trucks carry shipments of hazardous materials every day across the United States, according to the Department of Transportation. Chris Bertelli, deputy director of the California's Office of Homeland Security, said his agency will examine the economic fallout of Sunday's accident. Source: <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2007/05/01/MNGQUPII751.DTL>

14. *May 01, North Jersey Media Group* — **New Jersey is studying ways to manage traffic by charging those who create it.** New Jersey could be close to charging drivers to enter the Garden State. Faced with stifling traffic at river crossings, the Port Authority of New York and New Jersey is studying ways to manage traffic by charging those who create it. So-called "congestion pricing" could be coming to bridges and tunnels soon. The Port Authority's new study, funded by the federal government, weighs whether to end the free ride back to New Jersey, according to the Federal Highway Administration (FHWA). Drivers would pay to both enter and leave New York. The express E-ZPass system, which permits drivers to cruise past booths on the New Jersey Turnpike and Garden State Parkway, would be employed on the bridges and tunnels. The Port Authority would keep track of drivers who don't have E-ZPass by photographing their license plate. Those drivers would be sent a bill by mail. New York Mayor Bloomberg recently proposed the same system for his New York City congestion scheme. "There is a movement in this country that recognizes the costs of building highways is so expensive," Jeffrey M. Zupan, a consultant and senior fellow at the Regional Plan Association said.

Source: <http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFIZUVFeXkzJmZnYmVsN2Y3dnFIZUVFeXk3MTI2NTY3JnlyaXJ5N2Y3MTdmN3ZxZWVFRXI5Mg==>

15. *May 01, Associated Press* — **Trucker got license despite criminal past.** The driver who crashed a tanker loaded with gasoline and brought down a heavily trafficked highway overpass was given a commercial trucker's license despite a history of criminal convictions, including drug and burglary arrests, authorities said. James Mosqueda, 51, of Woodland, CA, also got a special hazardous materials endorsement last year from the federal Transportation Security Administration despite regulations that can disqualify applicants with multiple convictions. To get it, he had to undergo an FBI criminal history check and an intelligence background check. The elevated section of highway that funnels traffic from the Bay Bridge to a number of key freeways was destroyed early Sunday after flames from Mosqueda's overturned gas truck caused part of that overpass to collapse onto a road below. Authorities said drugs and alcohol were not factors in the crash, and that Mosqueda may have lost control because he was speeding from a refinery in Benicia to a gas station near the Oakland airport. He served two years and eight months in prison after a 1996 arrest for heroin possession in Sacramento County, court records show. His criminal rap sheet stretching back to 1981 includes arrests for burglary, felony drug charges and possession of stolen property.

Source: <http://www.modbee.com/local/story/13538477p-14142525c.html>

16. *April 30, Government Accountability Office* — **GAO-07-660: Aviation Security: Federal Efforts to Secure U.S.-Bound Air Cargo Are in the Early Stages and Could Be**

Strengthened (Report). The Department of Homeland Security (DHS) has primary responsibility for securing air cargo transported into the United States from another country, referred to as inbound air cargo, and preventing implements of terrorism from entering the country. The Government Accountability Office (GAO) examined (1) what actions DHS has taken to secure inbound air cargo, and how, if at all, these efforts could be strengthened; and (2) what practices the air cargo industry and foreign governments have adopted that could enhance DHS's efforts to strengthen inbound air cargo security, and to what extent DHS has worked with foreign governments to enhance their air cargo security efforts. To conduct this study, GAO reviewed relevant DHS documents, interviewed DHS officials, and conducted site visits to seven countries in Europe and Asia. GAO recommends that DHS develop a risk-based inbound air cargo security strategy; develop a systematic process to improve interagency communication; and analyze air cargo security practices used by air cargo industry stakeholders and foreign governments to determine their applicability to the United States. DHS generally concurred with GAO's recommendations. However, GAO has concerns that DHS's plans may not fully address these recommendations.

Highlights: <http://www.gao.gov/highlights/d07660high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-660>

17. *April 30, Department of Transportation* — U.S., Mexican trucks will begin cross-border demonstration program at same time. U.S. Department of Transportation Secretary Mary E. Peters on Monday, April 30, announced that U.S. trucks will begin operating in Mexico for the first time ever starting at the same time Mexican trucks begin operating north of the commercial border zone in the U.S. The Secretary noted that the improvements to the demonstration program are a result of recent conversations with the Mexican government and Congress. In February, the Department of Transportation announced a yearlong demonstration program to expand cross-border trucking operations with Mexico. The program is designed to eliminate the current cumbersome, outdated and costly system of moving freight across the border, and replace it with an efficient, transparent and safe cross-border trucking process. The program's safety developments have been guided by, but not limited to, requirements established by Congress in 2002. The Department's independent Inspector General has also certified that the program substantially meets eight criteria addressing inspector training, inspection facilities and the development of safety procedures. The elements of the trucking program are discussed in a Federal Register notice issued today. The Department is seeking comment over the next 30 days on the program.

The notice is available online at <http://www.fmcsa.dot.gov>

Source: <http://www.dot.gov/affairs/dot4307.htm>

18. *April 30, Government Technology* — U.S., Mexican officials announce opening of SENTRI in Brownsville, Texas. U.S. and Mexican officials came together in the middle of the Veteran's/Los Tomates International Bridge to announce the formal grand opening of the Secured Electronic Network Traveler Rapid Inspection Lane, also known as SENTRI. A ribbon-cutting ceremony signaled the formal launch of operations of the frequent traveler program. Following the playing of both nation's anthems, officials addressed the border operations in the growing region. SENTRI provides a dedicated lane and expedited U.S. Customs and Border Protection (CBP) processing for pre-approved, low-risk travelers. Applicants must voluntarily undergo a thorough biographical background check against criminal, law enforcement, customs, immigration, and terrorist indices, a 10-fingerprint law

enforcement check, and a personal interview with CBP. Once approved, a SENTRI participant is issued a Radio Frequency Identification Card (RFID) that will identify their record and status in the CBP database upon arrival at the U.S. port of entry. An RFID transponder is also issued to the applicant's vehicle.

Source: http://www.govtech.net/magazine/channel_story.php/105246

[\[Return to top\]](#)

Postal and Shipping Sector

19. *May 01, USPS News Release* — Mail internationally, domestically with one package. For the first time since 1995, the U.S. Postal Service's (USPS) familiar and trusted products for shipping domestically and internationally will have a new look. With a focus on convenience, the Postal Service has redesigned all Priority Mail and Express Mail packages and envelopes, including the popular Flat Rate boxes and envelopes. Mailers can use the same Priority Mail and Express Mail packaging whether they are shipping within the United States or to another country, beginning May 14. Express Mail and Priority Mail packages and envelopes remain available free of charge — as does package pickup. The Postal Service has taken additional steps to adding convenience for international mailers, simplifying the eight main International Mail products into four: Global Express Guaranteed, Express Mail International, Priority Mail International and First-Class Mail International.

Source: http://www.usps.com/communications/newsroom/2007/pr07_035.htm

[\[Return to top\]](#)

Agriculture Sector

Nothing to report.

[\[Return to top\]](#)

Food Sector

20. *April 30, U.S. Department of Agriculture* — Joint Update: FDA/USDA trace adulterated animal feed to poultry. The Department of Agriculture (USDA) and the Food and Drug Administration (FDA) have learned that byproducts from pet food manufactured with contaminated wheat gluten imported from China have been used in chicken feed on some farms in the state of Indiana. This information came to light as part of the continuing investigation into imported rice protein concentrate and wheat gluten that have been found to contain melamine and melamine-related compounds. At this time, the investigation indicates that approximately 30 broiler poultry farms and eight breeder poultry farms in Indiana received contaminated feed in early February and fed it to poultry within days of receiving it. All of the broilers believed to have been fed contaminated product have since been processed. The breeders that were fed the contaminated product are under voluntary hold by the flock owners. FDA and USDA believe the likelihood of illness after eating chicken fed the contaminated product is very low. Because there is no evidence of harm to humans associated with consumption of chicken fed the contaminated product, no recall of poultry products processed

from these animals is being issued. Testing and the joint investigation continue.

Additional information: <http://www.fda.gov/oc/opacom/hottopics/petfood.htm>

Source: http://www.usda.gov/wps/portal/!ut/p/s.7.0.A/7.0.1OB/.cmd/a.d/ar/sa.retrievecontent/c/6.2.1UH/.ce/7.2.5JM/.p/5.2.4TQ/.d/0/th/J.2.9D/s.7.0.A/7.0.1OB?PC.7.2.5JM.contentid=2007%2F04%2F0122.xml&PC.7.2.5JM.parentnav=LATEST_RELEASES&PC.7.2.5JM.navid=NEWS_RELEASE#7.2.5JM

21. *April 27, U.S. Department of Agriculture* — **Consumers should check refrigerators for potentially tainted cheeses.** Florida Agriculture and Consumer Services Commissioner Charles H. Bronson is urging consumers to check their refrigerators for Ole Mexican Foods' Verole Queso Fresco Authentic Mexican Crumbling Cheese and Ole Fresco Authentic Mexican Crumbling Cheese. The two products may be contaminated with E. coli bacteria. The potential for this contamination was determined after random testing performed by the Florida Department of Agriculture and Consumer Services revealed the presence of E.coli bacteria in samples of both of the cheeses.

Source: http://www.fda.gov/oc/po/firmrecalls/olemexican04_07.html

22. *April 25, U.S. Department of Agriculture* — **SmartPak Canine recalls LiveSmart Weight Management Formula.** SmartPak Canine used rice protein concentrate supplied by Wilbur–Ellis for a single, recently produced batch of its LiveSmart – Weight Management Formula dog food. SmartPak is voluntarily recalling that batch of the product. Virtually all of the potentially contaminated batch was recovered by SmartPak before going to customers; only 45 pet owners received shipments of the affected product and all of them have been contacted. SmartPak has not received any reports of pets taking ill as a result of feeding LiveSmart Weight Management food.

Source: http://www.fda.gov/oc/po/firmrecalls/smartpak04_07.html

[\[Return to top\]](#)

Water Sector

23. *April 30, Reuters* — **California snowpack supply seen lowest in 20 years.** California water officials said on Monday, April 30, they expect the water level in the Sierra Nevada mountains snowpack this year will be the lowest in almost 20 years, crimping supplies for hydropower and other water uses and raising concern about 2008. The California Department of Water Resources (DWR) will conduct its fifth and final snowpack survey of the winter season on Tuesday, but new figures point to about 29 percent of normal water content, down from 34 percent at the beginning of April. "The figures will be quite low, probably the lowest since 1988," said Don Strickland, a spokesperson for DWR. California depends on the snowpack to generate almost one–fifth of its electricity supplies, help irrigate the biggest agricultural economy in the United States, fill reservoirs, and support recreation on the state's rivers.

Source: <http://www.sciam.com/article.cfm?alias=california-snowpack-suppl&chanID=sa003&modsrc=reuters>

24. *April 30, Associated Press* — **Colorado river states file drought plan.** Seven states dependent

on the Colorado River filed a plan with the Interior Department on Monday, April 30, aimed at divvying up water resources during times of drought. Officials said the long-debated pact would protect 30 million people who depend on the river for drinking water. "The adversity of drought has brought the states together and forced us to rethink how we manage this precious resource," said George Caan, executive director of Nevada's Colorado River Commission. Under rules that date to the 1920s, the four upper Colorado River basin states of Colorado, New Mexico, Utah and Wyoming are obligated to let 8.23 million acre feet of water per year flow to three lower basin states – Arizona, California and Nevada. Under the proposed plan, the upper basin states could release less water downstream during a drought and if a less-than-average snowpack accumulates on the western slopes of the Rocky Mountains. The lower basin states would adjust through what the plan calls "intentionally created surpluses." For example, the Southern Nevada Water Authority would be able to tap water holdings in the Coyote Spring area of Nevada and exercise its rights to draw water from the Virgin and Muddy rivers. Source: <http://www.forbes.com/feeds/ap/2007/04/30/ap3670620.html>

25. *March 30, Government Accountability Office — GAO-07-480: Securing Wastewater Facilities: Costs of Vulnerability Assessments, Risk Management Plans, and Alternative Disinfection Methods Vary Widely (Report)*. Since September 11, 2001, the nation's water infrastructure has received greater attention, including the risk of terrorist attacks at wastewater facilities that store hazardous chlorine gas for disinfection. In 2006, the Government Accountability Office (GAO) reported that many large wastewater facilities have responded to this risk by voluntarily conducting vulnerability assessments and converting from chlorine gas to other disinfection methods. In this study, GAO was asked to provide information on (1) the range of costs large wastewater treatment facilities incurred in preparing vulnerability assessments and risk management plans, and (2) the costs large wastewater treatment facilities incurred in converting from chlorine gas to alternative disinfection processes. Among the large wastewater facilities GAO examined, the costs reported to prepare vulnerability assessments ranged from \$1,000 to \$175,000, while costs to prepare risk management plans ranged from less than \$1,000 to over \$31,000. For the large wastewater facilities GAO examined, reports of actual and projected capital costs to convert from chlorine gas to alternative disinfection methods range from about \$650,000 to just over \$13 million. Highlights: <http://www.gao.gov/highlights/d07480high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-480>

[\[Return to top\]](#)

Public Health Sector

26. *May 01, News-Medical.Net (Australia) — Protecting Americans against a smallpox outbreak*. In the event of a smallpox outbreak in the United States, how long would it take for a vaccine to start protecting Americans by stimulating an immune response? A new national study led by Saint Louis University School of Medicine will attempt to answer this question. General routine vaccinations for smallpox were stopped in the United States in 1971, and the world was declared free of smallpox in 1980. But because of the recent concern about biowarfare and bioterrorism throughout the world, the U.S. government is making efforts to improve its ability to protect its citizens in the event of a bioterrorist attack involving the smallpox virus (*Variola major virus*). This study at Saint Louis University will look at the

ability of an investigational vaccine made by Bavarian Nordic to stimulate the immune system against smallpox.

Source: <http://www.news-medical.net/?id=24477>

27. *May 01, Reuters* — Infants acquire pertussis from family members. Family members are responsible for more than three quarters of pertussis cases transmitted to infants, according to a new report. In the United States, the incidence of infant pertussis, or whooping cough, has tripled in the past two decades despite widespread vaccination coverage, leading the Advisory Committee on Immunization Practices (ACIP) to recommend that all adolescents and adults receive a pertussis booster shot. To get a better handle on precisely how infants are catching pertussis, Dr. Annelies Van Rie from University of North Carolina at Chapel Hill and associates collected comprehensive data on close contacts of a group of infants with laboratory-confirmed pertussis. Rie and colleagues say they found "robust evidence" that household members are responsible for 73 percent to 82 percent of whooping cough transmission to infants for whom a source case could be identified.

Source: <http://health.yahoo.com/news/174675: ylt=AscYZkiP2E90PnU6F6F VHmumxbAB>

28. *May 01, This Is Wiltshire (England)* — Two UK hospital wards quarantined due to two viruses. Patients in two Wiltshire, England, hospital wards have been quarantined after 55 people were struck down by two virulent viruses. The Great Western Hospital has had 39 patients and 16 staff suffering vomiting and diarrhea in the past month and has now closed 16 beds to stop infection spreading. Most of the infected patients are being treated in isolation, no new patients will be admitted to Neptune and Teal wards and transfers between wards have been put on hold. "There are two main bugs we are fighting at the moment. One is Clostridium Difficile which causes diarrhea and the other is a virus that causes diarrhea and vomiting. The bug is circulating in the community at the moment and has already affected a number of hospitals in the region," said Ruth McCarthy, Director of infection control.

Source: http://www.thisiswiltshire.co.uk/news/headlines/display.var.1365722.0.patients_laid_low_by_virus_outbreak.php

29. *April 30, Center for Infectious Disease Research & Policy* — New York group offers plan for rationing ventilators in pandemic. A hypothetical but not unlikely scenario: Amid an influenza pandemic, a small hospital has three patients who need mechanical ventilation. One has terminal cancer, another has severe chronic lung disease, and a third has a severe case of flu. With only one ventilator available, which patient will get it? When the next flu pandemic comes, it's a good bet that ventilators will run short and clinicians will face wrenching decisions like these. Expecting that such choices will be excruciating for already stressed healthcare workers, a group of experts assembled by the New York State Department of Health (NYSDOH) is offering guidelines for rationing scarce ventilators. Last month the group released a 52-page draft plan that provides detailed guidance for determining who will receive ventilator treatment in the face of a pandemic-related shortage. The plan calls for allocating ventilators in acute care hospitals solely on the basis of patients' medical need and chance of survival, without regard for age, occupation, ability to pay, or other factors. The task force, called the New York State Workgroup on Ventilator Allocation in an Influenza Pandemic, has invited public comments on the proposed guidelines and plans to revise them in coming months.

NYSDOH proposal: <http://www.health.state.ny.us/diseases/communicable/influenz>

[a/pandemic/ventilators/docs/ventilator_guidance.pdf](#)

Source: <http://www.cidrap.umn.edu/cidrap/content/influenza/panflu/news/apr3007ventilator.html>

30. *April 30, Sawf News (TX)* — **'Supermap' of avian flu to predict the next outbreak.** A team of biomedical experts, led by Daniel Janies of Ohio State University have designed a new, interactive map of the spread of the avian flu virus (H5N1) that for the first time incorporates genetic, geographic and evolutionary information that may help predict where the next outbreak of the virus is likely to occur. In the process, they also tested hypotheses about the nature of specific strains of the virus that appear to be heading westward and have the ability to infect humans. Researchers used special software to create an evolutionary tree of the virus's mutations. They used Keyhole Markup Language in Google Earth to project the tree onto the globe and then chose colors and symbols to indicate different hosts that carry the virus and where they live. TimeSpan, another function in Google Earth, allowed them to animate the spread of the virus over the past decade. The map is chock-full of additional information. Clicking on a specific viral subtype generates a pop-up window revealing diagnostic mutations that distinguish one strain of the virus from another, and all of the data is linked to the National Institute of Health's GenBank. The study is available for purchase: <http://www.informaworld.com/smpp/content?content=10.1080/10635150701266848>
Source: <http://news.sawf.org/Health/36499.aspx>

[[Return to top](#)]

Government Sector

31. *May 01, WUSA (DC)* — **College campus alerts.** University officials all over the country are re-assessing how they communicate emergencies to their communities. Prior to the Virginia Tech tragedy, only a handful of colleges and universities in the DC Metro area used text messaging to cell phones as a way to communicate with students and faculty. The University of Maryland in College Park, MD, has just signed up for a service and other schools tell 9NEWS NOW they are looking into it. "We have the ability to stop every other message in our system so that if we have an emergency that needs to go out it certainly takes priority," says Julie Green Bataille, a spokesperson for Georgetown University in Washington, DC. Georgetown is also one of a few campuses in the area that has an emergency siren. Some schools have police cars with loud speakers or bullhorns to relay information. In addition, Georgetown has a campus television station that can get information out. Several schools in the area also have internal radio stations.
Source: http://www.wusa9.com/news/news_article.aspx?storyid=58119
32. *May 01, San Francisco Chronicle* — **Mental health training to spot troubled students.** Two weeks after a disturbed student's killing spree at Virginia Tech in Blacksburg, VA, University of California– Berkeley is ramping up efforts to expand its training of faculty, staff and students in identifying and helping students in need of help. Nearly 600 people have already undergone the training and roughly 100 green stickers mark the campus doors and work spaces of some of those ready to help. Efforts are underway to increase the number of stickers and their visibility on the 34,000–student campus. "I think the Virginia Tech incident was a wake-up call to a lot of faculty and students that we're not really doing a very good job of

looking out for the distressed student," said Mary Ann Mason, UC–Berkeley's graduate division dean and co–chair of the chancellor's advisory committee on student mental health. As part of its "Look for the Signs" training program, the campus is planning a training symposium later this month on how to identify the warning signs of depression and other mood trouble in students — and what to do when a student needs help. One goal of the training is to create standards for all members of the campus community in identifying the warning signs of mood trouble and taking the first steps to aid a student.

Source: <http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2007/05/01/MNGOUIKHS1.DTL>

- 33. *April 24, Government Accountability Office* — **GAO–07–755T: Capitol Visitor Center: Update on Status of Project's Schedule and Cost as of April 17, 2007 (Reposted Testimony)**.** These remarks are based on the Government Accountability Office's (GAO) review of schedules and financial reports for the Capital Visitor's Center (CVC) project and related records maintained by the Architect of the Capital (AOC) and its construction management contractor; observations on the progress of work at the CVC construction site; and discussions with the CVC team, AOC's Chief Fire Marshal, and representatives from the U.S. Capitol Police. Since the March 13, 2007, CVC hearing, the CVC team has continued to move the project's construction forward, but AOC has extended the project's scheduled completion date by about two months, to June 2008, and further delays are possible. To date, AOC's implementation of actions identified in its November 2006 action plan has not been completely effective in curtailing additional schedule slippages. Furthermore, ongoing communication and coordination breakdowns between the contractors and AOC's Chief Fire Marshal, as well as the large number of proposed change orders (over 450 as of February 2007), continue to present risks to the project's completion time frames and costs. AOC has requested \$20 million in fiscal year 2008 CVC construction appropriations to cover remaining costs, and GAO estimates that AOC may need further appropriations in future fiscal years for construction changes and claims.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-755T>

[\[Return to top\]](#)

Emergency Services Sector

- 34. *April 30, Associated Press* — **FDNY drill tests wireless technology.**** Fire Department of New York (FDNY), technology, and Port Authority officials tested a new wireless system designed to give first responders fast access to video and other data during a fire drill on Sunday, April 29, at the World Trade Center site. Some 100 firefighters participated in Sunday's simulated fire at 7 World Trade Center, which stands in the shadows of ground zero in downtown Manhattan. The exercise included 20 mock injuries and a rescue from an elevator shaft, said Joseph Pfeifer, chief of counterterrorism for FDNY. Officials tested sending surveillance video from the building's 50th floor to the network operations center and from there to the fire department's operations center in Brooklyn, allowing them to monitor the scene remotely, Pfeifer said. The Port Authority of New York and New Jersey, which owns the trade center site, also participated in the drill.

Source: http://www.auburnpub.com/articles/2007/04/30/news/state/stat_e03.txt

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

35. *May 01, SC Magazine* — **Flaw in Winamp MP4 processing disclosed.** A hacker posted exploit code for a then-unknown vulnerability in the Winamp media player to the Milw0rm site on Monday, April 30. The flaw, which vendor eEye Digital Security ranked as "high" severity, allows an attacker to execute arbitrary code from a remote location, possibly taking full control of a system. Winamp, created by Nullsoft, is owned by AOL. The company said today that it is working to fix the flaw. The flaw exists in Winamp version 5.34, according to eEye. Secunia, which released an advisory for the vulnerability today, urged users to not open untrusted MP4 files and ranked the flaw as "highly critical."

Secunia advisory: <http://secunia.com/advisories/25089/>

eEye Digital Security: <http://research.eeye.com/html/alerts/zeroday/20070430.html>

Source: <http://scmagazine.com/us/news/article/654194/flaw-winamp-mp4-processing-disclosed/>

36. *April 30, Government Computer News* — **NIST issues RFID guidelines.** The National Institute of Standards and Technology (NIST) last week issued guidelines and a set of best practices for the use of radio frequency technology by federal agencies, as well as private corporations. NIST said entities deploying RFID technologies need to consider any security or privacy risks that could arise and should minimize those risks by following a list of best practices developed for RFID users. The guidelines focus specifically on the use of RFID technologies for asset management, tracking, matching and process and supply chain control. While RFID offers the potential for organizations to improve their logistics, reduce expenses and increase safety, it also entails the risk of eavesdropping and unauthorized use, according to NIST, an organization within the Commerce Department.

Guidelines for Securing Radio Frequency Identification Systems:

http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

Source: http://www.gcn.com/online/vol1_no1/43601-1.html

Internet Alert Dashboard

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

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.