



# Department of Homeland Security Daily Open Source Infrastructure Report for 13 July 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

- VNUNet reports utility companies could be facing a hacking time bomb owing to poor security measures, since as more utilities move control and billing systems online, hackers are increasingly turning their attention to the possibilities of controlling the systems. (See item [3](#))
- Congressional investigators set up a bogus company with only a postal box and within a month obtained a license from the Nuclear Regulatory Commission that allowed them to buy enough radioactive material for a small dirty bomb. (See item [4](#))
- The Associated Press reports two planes came within 100 feet of colliding at Fort Lauderdale–Hollywood International Airport on Wednesday, July 11, after one missed its turn onto a taxiway and entered the runway where the other was about to land. (See item [11](#))

### 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. *July 13, Associated Press* — **Attacks on Mexican gas line shut factories.** Honda, Hershey and other multinational companies temporarily shut down their factories in western Mexico on Wednesday, July 11, after rebels attacked a key natural gas pipeline. The small left-wing guerrilla group that claimed responsibility for the pipeline explosions issued a statement late

Tuesday vowing to continue the attacks, while the Mexican government scrambled to increase security at "strategic installations" across Mexico. Officials from Mexico's state-owned oil and gas monopoly Petroleos Mexicanos, or Pemex, said an explosion Tuesday and two more last week affected different sections of the same pipeline extending from central Mexico City to Guadalajara, the industry-rich capital of the western state of Jalisco. At least a dozen companies including Grupo Modelo SA, Mexico's largest beer maker, were forced to suspend or scale back operations because of the lack of natural gas. The blast in the central state of Querétaro damaged a 36-inch pipeline, cutting supplies to the cities of Guadalajara, Querétaro, Aguascalientes and Leon. Pemex said the gas would probably not be restored until Friday at the earliest, but was working to provide alternative means of delivery.

Source: [http://seattletimes.nwsourc.com/html/nationworld/2003785485\\_mexgas12.html](http://seattletimes.nwsourc.com/html/nationworld/2003785485_mexgas12.html)

2. *July 12, News & Observer (NC)* — **GAO to examine enforcement of fire safety at nuclear plants.** The Government Accountability Office (GAO) has agreed to review fire safety enforcement at the nation's nuclear power plants, including Progress Energy's Shearon Harris nuclear plant in Wake County. GAO will begin the safety review in September at the behest of U.S. Rep. David Price (D-NC). Price's congressional district includes Progress Energy's Shearon Harris nuclear plant. Fire walls and fire retardants at the plant have sometimes failed standards since 1989, two years after the plant began operating. The NRC said five years ago that 6,500 feet of electrical cable at Shearon Harris does not meet federal fire safety standards, but the NRC is allowing the power plant to use interim safety measures until the problem is fixed in late 2010. The electrical cable — required to operate emergency equipment — is wrapped in fireproof insulation that did not withstand intense heat under laboratory conditions. The goal of the GAO study is to reassure the public that the NRC's oversight of nuclear fire safety is adequate, or to point out deficiencies and suggest improvements.

Source: <http://www.newsobserver.com/politics/story/634523.html>

3. *July 12, VNUNet* — **Utility firms sitting on hacking time bomb.** Utility companies could be facing a hacking time bomb owing to poor security measures. As more utilities move control and billing systems online an analyst has warned that hackers are increasingly turning their attention to the possibilities of controlling the systems. While there is little direct financial benefit in breaking into such systems, there may be other benefits. "The utility companies are moving to completely digital systems and security is not prioritized," said Fran Howarth of Hurwitz & Associates. "Hackers could siphon off electricity for use in projects like indoor drug farms, for example, and charge it to consumers. "The problem is that 80 to 90 percent of the critical infrastructure is in private hands and they have their own security problems, so consumers are low down on the list."

Source: <http://www.vnunet.com/vnunet/news/2194040/utilities-sitting-hacking-bomb>

4. *July 11, Associated Press* — **Bogus company gets radioactives' license.** Congressional investigators set up a bogus company with only a postal box and within a month obtained a license from the Nuclear Regulatory Commission (NRC) that allowed them to buy enough radioactive material for a small "dirty bomb." Senator Norm Coleman (R-MN) said the sting operation raises concerns about terrorists obtaining such material just as easily. Nobody at the NRC checked whether the company was legitimate and an agency official even helped the investigators fill out the application form, Coleman said Wednesday. The NRC acknowledged that more checking is needed in such licensing and said that since being told of the Government

Accountability Office sting operation it has tightened licensing procedures. "We've fixed the problem," said NRC Commissioner Edward McGaffigan on Wednesday. He said that such licenses now will require visits to the company or in some cases company officials will have to come to NRC offices. The license that was obtained allowed for the purchase of up to five portable moisture density gauges widely used in construction, in which are encased small amounts of cesium-137 and americium 241, two highly radioactive isotopes.

Source: [http://news.yahoo.com/s/ap/20070711/ap\\_on\\_go\\_ot/dirty\\_bomb\\_2](http://news.yahoo.com/s/ap/20070711/ap_on_go_ot/dirty_bomb_2)

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

## **Chemical Industry and Hazardous Materials Sector**

5. *July 12, Star-Ledger (NJ)* — **Lightning sets refinery tank on fire.** A large chemical storage tank at a Sunoco refinery in South Jersey was struck by lightning and set ablaze Wednesday afternoon, July 11, shooting flames hundreds of feet into the air and darkening the sky with vast plumes of black smoke. Firefighters from across Gloucester County were called in to battle the four-alarm blaze at the Coastal Eagle Point Refinery along the Delaware River in West Deptford Township. Gerald Davis, a spokesperson for Philadelphia-based Sunoco Oil Co., said the fire never posed a hazard to area residents. The white cylindrical tank contained 1.5 million gallons of Xylene. Air testing showed no contamination in surrounding neighborhoods, though residents were urged to remain indoors. Traffic backed up in the immediate area after police shut down Route 130, forcing vehicles onto jammed side roads.

Source: <http://www.nj.com/news/ledger/jersey/index.ssf?base/news-7/118421612887740.xml&coll=1>

6. *July 11, Associated Press* — **Ammonia leak prompts evacuation.** A white cloud of anhydrous ammonia at least 100 feet across and 35 feet tall sparked evacuations in northeast Sidney, NE, Wednesday, July 11. Officials say the ammonia came from Farmers Elevator Company in northeast Sidney. Residents in the northeast part of town were evacuated from outside areas, and other residents were asked to stay indoors with windows closed.

Source: <http://www.kolnkgin.com/grandisland/headlines/8443262.html>

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

## **Defense Industrial Base Sector**

7. *July 13, Government Accountability Office* — **GAO-07-836: Unmanned Aircraft Systems: Advance Coordination and Increased Visibility Needed to Optimize Capabilities (Report).** Combatant commanders carrying out ongoing operations rank the need for intelligence, surveillance, and reconnaissance (ISR) capabilities as high on their priority lists. The Department of Defense (DoD) is investing in many ISR systems, including unmanned aircraft systems (UAS), to meet the growing demand for ISR assets to support the warfighter. The Government Accountability Office (GAO) was asked to evaluate DoD's efforts to integrate UAS into ongoing operations while optimizing the use of all DoD ISR assets. Specifically, this report addresses the extent that (1) DoD has taken steps to facilitate the integration of UAS into combat operations, and (2) DoD's approach to allocating and tasking its ISR assets considers all

available ISR capabilities, including those provided by UAS. GAO also reviewed the extent that DoD evaluates the performance of its ISR assets, including UAS, in meeting warfighters' needs. To perform this work, GAO analyzed data and guidance on the use of ISR assets, and interviewed DoD officials, including those supporting ongoing operations in Iraq and Afghanistan.

Highlights: <http://www.gao.gov/highlights/d07836high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-836>

8. *July 10, Government Accountability Office — GAO-07-1064T: DoD's High-Risk Areas: Efforts to Improve Supply Chain Can Be Enhanced by Linkage to Outcomes, Progress in Transforming Business Operations, and Reexamination of Logistics Governance and Strategy (Testimony)*. The availability of spare parts and other critical items provided through the Department of Defense's (DoD) supply chains affects the readiness and capabilities of U.S. military forces. Since 1990, the Government Accountability Office (GAO) has designated DoD supply chain management as a high-risk area. In 2005, DoD developed a plan aimed at addressing supply chain problems and having GAO remove this high-risk designation. DoD's plan focuses on three areas: requirements forecasting, asset visibility, and materiel distribution. GAO was asked to provide its views on (1) DoD's progress in developing and implementing the initiatives in its plan, (2) the results of recent work relating to the three focus areas covered by the plan, and (3) the integration of supply chain management with efforts to improve defense business operations. GAO also addressed broader issues of logistics governance and strategic planning. This testimony is based on prior GAO reports and analysis. To determine whether to retain the high-risk designation for supply chain management, GAO considers factors such as whether DoD makes substantial progress implementing improvement initiatives; establishes a program to validate the effectiveness of the initiatives; and completes a comprehensive, integrated strategy.

Highlights: <http://www.gao.gov/highlights/d071064thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-1064T>

9. *June 29, Government Accountability Office — GAO-07-807: Defense Logistics: Efforts to Improve Distribution and Supply Support for Joint Military Operations Could Benefit from a Coordinated Management Approach (Report)*. During Operation Iraqi Freedom, the Army and the Marine Corps experienced problems with the delivery of supplies to the warfighter. Such problems highlight long-standing weaknesses in the Department of Defense's (DoD) supply chain management. DoD has identified joint theater logistics as a key effort aimed at improving distribution and supply support. The Government Accountability Office (GAO) was asked to examine DoD's efforts to develop and implement joint theater logistics. GAO assessed (1) the extent to which DoD's approach to managing joint theater logistics departmentwide encompasses sound management principles and (2) the progress DoD has made in implementing joint theater logistics initiatives. GAO reviewed DoD documents and interviewed officials from the Joint Staff, services, agencies, and geographic combatant commands. GAO recommends DoD develop and implement a coordinated and comprehensive management approach to guide and oversee efforts across the department to improve distribution and supply support to U.S. forces in a joint theater. GAO also recommends that DLA assess opportunities to consolidate storage and shipping activities within all geographic combatant commands. DoD concurred with GAO's recommendations.

Highlights: <http://www.gao.gov/highlights/d07807high.pdf>

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

## **Banking and Finance Sector**

10. *July 12, Computerworld Australia* — **Bootable disc eliminates viruses for safer banking.** A computer science researcher has developed a secure software application intended to bypass the problem of viruses altogether. "Viruses are a fact of life. Let's provide a different way of doing certain things which are not affected by viruses," says Professor Paddy Krishnan of Bond University. Krishnan and his team at Bond's Software Assurance Center in Australia have created a secure platform for computing in the form of a live CD. The software, tentatively entitled BOSS (Bank on Secure System), was designed with the home-user in mind and is limited to specific applications that involve sensitive transactions, such as e-banking. Krishnan claims the procedure is easy. The end-user simply slips the CD into the PC and reboots it. Instead of the usual operating system loading at boot, the BOSS loads first. Once loaded a browser opens followed by a graphical keyboard for added security. Normal online banking can then be conducted on this secure platform. When the user completes her transaction the original operating system is restored by simply removing the CD and rebooting. "The advantage of this [technology] is that when you're doing your banking the viruses that live on your hard-drive are not active anymore."

Source: [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026889&intsrc=news\\_ts\\_head](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026889&intsrc=news_ts_head)

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

## **Transportation and Border Security Sector**

11. *July 12, Associated Press* — **Two planes nearly collide on Florida runway.** Two planes came within 100 feet of colliding at Fort Lauderdale-Hollywood International Airport after one missed its turn onto a taxiway and entered the runway where the other was about to land, federal authorities said. Air traffic controllers noticed a plane entering a runway Wednesday, July 11, as Delta Flight 1489 approached the same runway for a landing, Federal Aviation Administration (FAA) spokesperson Kathleen Bergen said. The controllers alerted the Delta crew to pull up and circle the airport to avoid United Flight 1544, which had missed a turn onto another taxiway, Bergen said. Investigators were focusing on what caused the United flight to veer into Delta's right of way, Bergen said. The near-miss, or "runway incursion" in FAA terminology, is under investigation.

Source: [http://biz.yahoo.com/ap/070712/planes\\_near\\_collision.html?v=1](http://biz.yahoo.com/ap/070712/planes_near_collision.html?v=1)

12. *July 12, Associated Press* — **Flight diverted over passenger scare.** A flight from Los Angeles to London was diverted to New York Thursday, July 12, because of what officials said may have been an unfounded security scare. A flight attendant on the American Airlines plane became concerned that a passenger might not have gone through proper security screening before boarding the Heathrow Airport-bound flight at Los Angeles International Airport, said airline spokesperson Sonja Whitemon. The flight attendant had seen the male passenger ride to

the terminal on an employee bus and bypass security, as employees are able to do, Whitemon said. After talking to the passenger, flight crewmembers decided they needed to divert the plane to New York's John F. Kennedy International Airport to search the cabin and re-screen the 230 passengers, in keeping with standard security procedures, she said. Whitemon said she could not confirm whether the passenger was an airline employee. Authorities were questioning the passenger Thursday morning at Kennedy airport, officials said.

Source: [http://biz.yahoo.com/ap/070712/flight\\_diverted.html?.v=1](http://biz.yahoo.com/ap/070712/flight_diverted.html?.v=1)

13. *July 12, Associated Press* — **Amtrak president: High-speed rail would cost billions.** Even if it spent \$7 billion on track upgrades, Amtrak couldn't reduce the travel time between Washington and New York to less than two hours and 20 minutes, which is only 25 minutes less than the trip now takes, the company's president, Alex Kummant, told Congress on Wednesday, July 11. During the hearing, members of the House transportation committee expressed frustration about the lack of truly high-speed rail service in the U.S. The closest thing Amtrak has to high-speed service is the Acela Express, the railroad's premier Washington-Boston train, which travels at an average speed of 82 miles per hour and reaches 150 mph in parts of Rhode Island and Connecticut. In other parts of the country, where Amtrak runs trains on congested tracks owned by the freight railroads, speeds can be far slower and delays are frequent. But even on the northeast corridor, it would be impossible to maintain speeds of 125 to 150 mph on the entire route using the current infrastructure, which Amtrak shares with numerous commuter lines and some freight carriers, Kummant has said. Such speeds — which could cut the trip from Washington to New York down to about an hour and a half — would require a dedicated line, Kummant said.

Source: [http://www.usatoday.com/travel/news/2007-07-11-amtrak-high-speed\\_N.htm](http://www.usatoday.com/travel/news/2007-07-11-amtrak-high-speed_N.htm)

14. *July 12, Government Accountability Office* — **GAO-07-1104T: Federal Aviation Administration: Viability of Current Funding Structure for Aviation Activities and Observations on Funding Provisions of Reauthorization Proposals (Testimony).** The Federal Aviation Administration (FAA) operates one of the safest air transportation systems in the world, but this system is under growing strain as the demand for air travel increases. Recognizing the need to transform this system, Congress created the Joint Planning and Development Office, housed within FAA, to plan and develop the Next Generation Air Transportation System (NextGen). The current authorization for FAA, the Airport and Airway Trust Fund (Trust Fund), and the excise taxes that support the Trust Fund will expire September 30, 2007. Reauthorization bills in the Senate (S. 1300) and the House (H.R. 2881) identify various revenue sources, including flight surcharges and certain fees, to fund FAA, including NextGen. Concerned about the need for stable, sustainable financing for the nation's multibillion-dollar transportation infrastructure investments, including NextGen, the Government Accountability Office (GAO) has designated transportation financing as high risk. GAO's statement addresses (1) the extent to which the current funding structure can support FAA's activities, including NextGen, (2) the implications of selected provisions of proposals to fund aviation activities, and (3) issues that could affect the overall cost of NextGen. The statement is based on recent GAO reports and testimonies, updated through interviews with FAA officials and stakeholder representatives.

Highlights: <http://www.gao.gov/highlights/d071104thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-1104T>

15. *July 12, WUSA9 (DC)* — **Big development plans may threaten small Virginia airport.** Pilots and owners of small planes are worried about a new housing development planned on the edge of Leesburg Executive Airport. They fear that once people move in, they will start complaining about the noise and force Loudoun County officials to shut the airport down. Aviation experts say the construction of new housing is one of the leading threats to small airports across the country. A final vote of Leesburg Town officials, along with the Loudoun County Board of Supervisors and executives, which was scheduled for next Tuesday, has now been postponed until September. The Aircraft Owners and Pilots Association has lobbied against the development.

Source: [http://www.wusa9.com/news/news\\_article.aspx?storyid=60695](http://www.wusa9.com/news/news_article.aspx?storyid=60695)

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

## **Postal and Shipping Sector**

16. *July 12, New York Times* — **United Parcel Service is going high tech.** At Worldport, the United Parcel Service (UPS) hub at the airport in Louisville, KY, workers typically have less than four hours to process more than a million packages from at least 100 planes and probably 160 trucks. Increasingly, it is the researchers at UPS' Atlanta headquarters, its technology center in Mahwah, NJ, and its huge four-million-square-foot Louisville hub who are asking the questions that will drive the company's future: What if the package contains medicine that could turn from palliative to poison if the temperature wavers? What if it is moving from Bangkok to Bangor and back to Bangkok, and if customs rules differ on each end? And what if the package is going to a big company that insists on receiving all its packages, no matter who ships them, at the same time each day? Increasingly, it is the search for high-tech answers to such questions that is occupying the entire package delivery industry. And now the UPS researchers are working on sensors that can track temperatures of packages, on software that can make customs checks more uniform worldwide and on scheduling processes that accommodate the needs of recipients as well as shippers.

Source: [http://news.com.com/Still+brown%2C+but+going+high+tech/2100-1022\\_3-6196227.html?tag=nefd.top](http://news.com.com/Still+brown%2C+but+going+high+tech/2100-1022_3-6196227.html?tag=nefd.top)

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

## **Agriculture Sector**

17. *July 11, Times Argus (VT)* — **New rule requires identification of Vermont sheep, goats.** Effective July 15, a new rule requiring the identification of sheep and goats when the animals are moved from the farm for sale or exhibition will be in effect in Vermont. "This rule is in response to the U.S. Department of Agriculture's (USDA) request for states to comply with requirements for the USDA's Accelerated Scrapie Identification Program, said Vermont State Veterinarian Kerry. The identification makes it possible to trace an animal to the farm where it was born, in case scrapie infection is detected later in the animal. Scrapie is a degenerative and eventually fatal disease affecting the central nervous system of sheep and sometimes goats.

Source: <http://www.timesargus.com/apps/pbcs.dll/article?AID=/20070711/THISJUSTIN/70711009>

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

## **Food Sector**

**18. *July 12, Food Safety and Inspection Service* — FSIS publishes final rule prohibiting processing of downer cattle.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) Thursday, July 12, announced a permanent prohibition on the slaughter of cattle that are unable to stand or walk (downer cattle) when presented for pre-slaughter inspection. The inability to stand or walk can be a clinical sign of Bovine Spongiform Encephalopathy (BSE). Under the rule, cattle that are injured after they pass pre-slaughter inspection will be reevaluated to determine their eligibility for slaughter. Veal calves that cannot stand because they are tired or cold may be set apart and held for treatment and re-inspection. The rule published in the July 13 Federal Register makes permanent what had been an interim final rule prohibiting slaughter of non-ambulatory cattle in the U.S. The final rule becomes effective October 1, 2007.

Source: [http://www.fsis.usda.gov/News & Events/NR\\_071207\\_01/index.as p](http://www.fsis.usda.gov/News_&_Events/NR_071207_01/index.as.p)

**19. *July 12, Associated Press* — E. coli made Colorado inmates sick.** E. coli is to blame for the outbreak of food-borne illness among dozens of inmates at a county jail, sheriff's officials said. About 70 Jefferson County, CO, inmates have reported symptoms including severe abdominal cramping, diarrhea, vomiting and a low-grade fever. Officials said that 37 inmates were still ill and that one was hospitalized Wednesday, July 11. County health officials were awaiting further test results to determine what strain of E. coli made the inmates ill, said Mark Johnson, head of the health department. Health officials were trying to determine what food might have been contaminated and how.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/12/AR2007071200050.html>

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

## **Water Sector**

**20. *July 12, Seattle Post-Intelligencer* — Washington state seeks new way to gauge Sound health.** Washington's fleet of ferries thrill legions of tourists, haul thousands of commuters and now — they're being eyed as future guardians of Puget Sound. The green-and-white vessels would be fitted with testing devices to continuously sample water quality, making the flotilla of ferries an early-warning system for everything from harmful algal blooms to oil and sewage spills. The plan is gaining traction in Washington, DC, and Seattle, with informal discussions earlier this week between Washington State Ferries and researchers at the University of Washington. "It's a fantastic idea," said Carol Maloy, who leads the state Department of Ecology's marine monitoring team. Maloy now runs the most extensive monitoring program for the Sound. The program relies on a seaplane hopscotching from Olympia to Bellingham, stopping between 40 different rotating locations to test the water. Seaplane sampling has been done for the past 35 years, but the method has its limitations. The planes can't be used when it's windy, foggy or dark — creating occasional gaps in the data. And the testing is done only once

a month. With ferries taking samples day and night, the picture would become much clearer. Problem spots would be quickly identified, toxic algal blooms could be tracked and scientists would gain an understanding of conditions they form in.

Source: [http://seattlepi.nwsource.com/transportation/323339\\_ferry12.html](http://seattlepi.nwsource.com/transportation/323339_ferry12.html)

**21. July 11, Atlanta Journal–Constitution — Vandals release one million gallons of water from hydrants.** Authorities say vandals released at least one million gallons of water from 15 fire hydrants in Heard, GA. County Water Authority director Jimmy Knight said the suspects may face up to 10 years in prison because federal Homeland Security laws prohibit tampering with a public utility.

Source: [http://www.ajc.com/news/content/metro/stories/2007/07/11/hydrants\\_0711.html](http://www.ajc.com/news/content/metro/stories/2007/07/11/hydrants_0711.html)

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

## **Public Health Sector**

**22. July 12, Reuters — Czechs confirm bird flu at two more farms.** Tests confirmed the H5N1 type of the bird flu virus in poultry at two farms in the eastern Czech Republic, the State Veterinary Authority (SVS) said on Thursday, July 12. The virus was found at the two farms with 71,000 poultry, bringing the number of outbreaks at Czech farms to four. Vets were preparing to cull all birds on the farms on Thursday, spokesperson Josef Duben said. The Czechs found their first bird flu case, which involved the lethal H5N1 strain, at a turkey farm in the eastern part of the country in June.

Source: <http://www.reuters.com/article/healthNews/idUSL1254558720070712>

**23. July 12, Associated Press — Equipment missing from CDC.** Last month, a congressional oversight committee requested an audit of the U.S. Centers for Disease Control and Prevention's (CDC) property management procedures and an investigation into allegations of theft at the center. CDC officials said they have accounted for about nine million dollars in missing goods in recent weeks. The committee specifically said it was concerned about a suspected "insider" burglary of \$500,000 in computers, and millions of dollars worth of other items missing or unaccounted for since the CDC's last audit in 1995. Between fiscal 2004 and 2006, there were 61 investigations into the theft or disappearance of CDC property. No arrests or disciplinary action resulted from those investigations, and several are ongoing, CDC spokesperson Tom Skinner said.

Source: <http://www.foxnews.com/wires/2007Jul12/0,4670,CDCMissingEquipment,00.html>

**24. July 12, Agence France–Presse — Dengue deaths in Cambodia this year exceed 2006 toll.** Dengue fever deaths in Cambodia so far this year have eclipsed fatalities in 2006 as the country battles one of the worst outbreaks of the disease in a decade, medical officials said Thursday, July 12. Some 182 fatalities have been recorded for the first half of this year out of 14,986 cases, said Ngan Chantha, director of the health ministry's dengue program. Last year 152 deaths were reported. Medical staff have been sent to the countryside to reinforce poorly equipped and staffed rural clinics. Dengue fever is on the rise around Southeast Asia with neighboring Thailand recording 19,000 cases and 18 deaths so far this year. Singapore has seen 4,029 cases and three deaths.

Source: [http://news.yahoo.com/s/afp/20070712/hl\\_afp/cambodiahealthiliness\\_070712100516](http://news.yahoo.com/s/afp/20070712/hl_afp/cambodiahealthiliness_070712100516)

25. *July 11, Associated Press* — **TB patient flees quarantine.** A man placed in isolation after he was diagnosed with contagious tuberculosis (TB) broke a hospital window and fled, health officials said. Franklin Greenwood was placed in isolation at the University of Arkansas for Medical Sciences (UAMS) hospital on June 29 after he was seen coughing up blood outside the city's traffic court. He left the hospital on July 1. UAMS spokesperson Leslie Taylor said the hospital had no authority to detain Greenwood but kept a civilian worker outside his room. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/11/AR2007071100823.html>

26. *July 11, Agence France-Presse* — **Indonesian bird flu victim had no contact with poultry.** A six-year-old Indonesian boy who died of bird flu last weekend had no apparent contact with poultry, an agriculture ministry official said Wednesday, July 11. The boy from Cilegon in Banten province, just west of the capital Jakarta, was Indonesia's 81st bird flu victim. Contact with infected birds is the most common form of transmission of the deadly virus to humans, experts say. Memed Zulkarnaen, director of the agriculture ministry's bird flu unit, said no infected poultry had been found within a radius of up to 300 yards from the boy's home. "The Indonesian medical community is still puzzled and does not understand from which source the victim was infected with the bird flu virus," he said. Source: [http://news.yahoo.com/s/afp/20070711/hl\\_afp/healthfluindonesia\\_070711173138;\\_ylt=AoQHigEAAtGo\\_2a93ubE9otKJOrgF](http://news.yahoo.com/s/afp/20070711/hl_afp/healthfluindonesia_070711173138;_ylt=AoQHigEAAtGo_2a93ubE9otKJOrgF)

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

## **Government Sector**

27. *July 12, Government Accountability Office* — **GAO-07-1075T: Critical Infrastructure: Sector Plans Complete and Sector Councils Evolving (Testimony).** As Hurricane Katrina so forcefully demonstrated, the nation's critical infrastructures -- both physical and cyber -- have been vulnerable to a wide variety of threats. Because about 85 percent of the nation's critical infrastructure is privately owned, it is vital that public and private stakeholders work together to protect these assets. The Department of Homeland Security (DHS) is responsible for coordinating a national protection strategy and has promoted the formation of government and private councils for the 17 infrastructure sectors as a collaborating tool. The councils, among other things, are to identify their most critical assets, assess the risks they face, and identify protective measures in sector-specific plans that comply with DHS's National Infrastructure Protection Plan. This testimony is based primarily on the Government Accountability Office's (GAO) July 2007 report on the sector-specific plans and the sector councils. Specifically, it addresses (1) the extent to which the sector-specific plans meet requirements, (2) the council members' views on the value of the plans and DHS's review process, and (3) the key success factors and challenges that the representatives encountered in establishing and maintaining their councils. GAO reviewed nine of the 17 draft plans and conducted interviews with government and private sector representatives.

Highlights: <http://www.gao.gov/highlights/d071075thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-1075T>

**28. *July 11, Department of Transportation* — Partnering to make school bus safety even safer.**

Department of Transportation Secretary Mary E. Peters on Wednesday, July 11, called on state and local governments, education officials, school bus manufacturers, safety advocates and consumer organizations to help the federal government assess the effectiveness of seat belts on school buses. Secretary Peters kicked off a daylong public meeting on the safety benefits, economic factors and other issues related to requiring seat belts on large school buses. Current federal standards for large school buses provide protection by the concept of compartmentalization, which does not require seat belts but creates a protection system like eggs in a carton. Compartmentalization combines flexible, energy-absorbent, high seat backs found on school buses and narrow spacing between each row to create a compartment that confines the occupant during a crash. Peters called on the meeting attendees to explore the best way to improve the safety of students riding on our nation's school buses. She noted, "We owe it to our children to look at this issue with fresh eyes. With that in mind, it's time to look at seat belts on buses," she added.

Source: <http://www.dot.gov/affairs/nhtsa1007.htm>

[[Return to top](#)]

## **Emergency Services Sector**

**29. *July 12, Federal Emergency Management Agency* — New USGS vehicle for emergency**

**response.** The U.S. Geological Survey (USGS) Wetlands Research Center in Lafayette, LA, are getting ready to help with search and rescue efforts, should they be needed. Lafayette is in a hurricane zone and the agency wanted to have the vehicle in a place where it can respond quickly. Inside the USGS vehicle is half a million dollars worth of potentially life-saving technology. The self-sustaining mobile unit serves as communications command post in crisis situations. The unit is equipped with a satellite phone in case there's no cell phone service, satellite Internet, and a single-side band marine radio. USGS workers can make and print out maps which can help out with search and rescue.

Source: <http://www.fema.gov/emergency/reports/2007/nat071207.shtm>

**30. *July 11, Occupational Health and Safety* — First responders to get electronic access to**

**Hazmat information, thanks to DOT, HHS.** According to the Department of Transportation (DOT), the 2008 Emergency Response Guidebook is the go-to reference for first responders to help them quickly identify hazardous material classifications, determine the best response, and protect themselves and the public immediately after an incident. Now, because of a joint effort between DOT and the Department of Health and Human Services (HHS), responders will for the first time have electronic access to the guidebook's information through laptops and PDAs for potentially even faster fact finding. Signed in late June, an agreement between the DOT Pipeline and Hazardous Materials Safety Administration and the HHS National Library of Medicine led to the development of a special software application called the Wireless Information System for Emergency Responders, which makes the electronic guidebook accessible through palm devices, some phones, and Windows-based laptops and desktops.

Source: <http://www.ohsonline.com/articles/49081/>

**31. *July 11, Seattle Times* — Cell phones and 911: patching a risky gap.** Emergency dispatchers receive an increasing number of calls from cell phones each year. Of the nearly 2.2 million calls

received by King County, WA, 911 dispatchers last year, about 1.3 million were from wireless callers. When a 911 dispatcher receives an emergency call from a regular telephone, or land line, the caller's phone number and address are automatically displayed on the operator's computer screen. But when the caller uses a cell phone, emergency-call-center dispatchers have only an approximate location of the source of the call. As a result, police, medics and firefighters might not be dispatched as quickly to life-threatening emergencies as they would be for calls made on a land line. King County's 911 call centers, and nearly every other urban emergency-dispatch center across the nation, are in the midst of upgrading dispatch systems to address the problems associated with the growing number of emergency calls made on cell phones. Once the technological upgrades are completed by 2009, the county's 911 centers will be able to use location software to accurately pinpoint cell phone callers. The goal is to come within nine meters of the source of a call.

Source: [http://seattletimes.nwsourc.com/html/localnews/2003783971\\_dispatch11m.html](http://seattletimes.nwsourc.com/html/localnews/2003783971_dispatch11m.html)

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

## **Information Technology and Telecommunications Sector**

- 32. July 12, U.S. Computer Emergency Readiness Team — US-CERT Technical Cyber Security Alert TA07-193A: Apple releases security updates for QuickTime.** Apple QuickTime contains multiple vulnerabilities. Exploitation of these vulnerabilities could allow a remote attacker to execute arbitrary code or cause a denial-of-service condition. Solution: Upgrade QuickTime Upgrade to QuickTime 7.2. This and other updates for Mac OS X are available via Apple Update.

Apple Update: <http://docs.info.apple.com/article.html?artnum=106704>

QuickTime 7.2: <http://www.apple.com/quicktime/download/>

On Microsoft Windows, QuickTime users can install the update by using the built-in auto-update mechanism, Apple Software Update, or by installing the update manually.

Apple Software Update: <http://docs.info.apple.com/article.html?artnum=304263>

An attacker may be able to exploit some of these vulnerabilities by persuading a user to access a specially crafted media file with a Web browser. Disabling QuickTime in your Web browser may defend against this attack vector. For more information, refer to the Securing Your Web Browser document. An attacker may be able to exploit some of these vulnerabilities by persuading a user to access a specially crafted Java applet with a Web browser. Disabling Java in your Web browser may defend against this attack vector. Instructions for disabling Java can be found in the Securing Your Web Browser document.

Securing Your Web Browser: [http://www.us-cert.gov/reading\\_room/securing\\_browser/](http://www.us-cert.gov/reading_room/securing_browser/)

Source: <http://www.us-cert.gov/cas/techalerts/TA07-193A.html>

- 33. July 11, eWeek — The 'zero-day' solution.** There's still no consensus regarding whether the zero-day vulnerability that security researcher Thor Larholm found is on Internet Explorer or on Firefox. But more to the point, there is a way to block the exploit, which otherwise could lead to remote system hijacking. According to Microsoft Security Program Manager Jesper Johansson, blocking the exploit boils down to deleting Firefox protocol handlers. To do so on a single computer, he said, requires running these commands: `reg delete HKCR\FirefoxHTML /f`; `reg delete HKCR\FirefoxURL /f`; and `reg delete HKCR\Firefox.URL /f`. One way to kill the protocol handlers on multiple machines is to group policy script and SMS packages, he said.

Rolling the fix out to thousands of machines can be done by creating a batch file deployed as a startup script. To enable restoration of the protocol handlers, Johansson recommended running this command on any machine with Firefox installed: `reg export HKCR\ backup.reg`. "That will create a reg script that you can use to re-import the settings once Mozilla produces a patch to fix the problem," he said.

Source: <http://www.eweek.com/article2/0.1895.2157333.00.asp>

- 34. July 11, U.S. Computer Emergency Readiness Team — US-CERT Technical Cyber Security Alert TA07-192A: Adobe Flash Player updates for multiple vulnerabilities.** There are critical vulnerabilities in Adobe Flash player and related software. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial-of-service on a vulnerable system. Systems affected: Microsoft Windows, Apple Mac OS X, Linux, Solaris, or other operating systems with any of the following Adobe products installed: Flash Player 9.0.45.0; Flash Player 9.0.45.0 and earlier network distribution; Flash Basic; Flash CS3 Professional; Flash Professional 8, Flash Basic; Flex 2.0; Flash Player 7.070.0 for Linux or Solaris. Solution: Apply Updates: Check with your vendor for patches or updates. For information about a specific vendor, please see the Systems Affected section in the vulnerability notes or contact your vendor directly. If you get the flash player from Adobe, see the Adobe Get Flash page for information about updates. Vulnerability notes: <http://www.kb.cert.org/vuls/id/945060>  
Adobe Get Flash: [http://www.adobe.com/shockwave/download/download.cgi?P1\\_Prod\\_Version=ShockwaveFlash](http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash)  
Disable Flash: Users who are unable to apply the patch should disable Flash.  
Adobe Security Bulletin: <http://www.adobe.com/support/security/bulletins/apsb07-12.html>  
Source: <http://www.uscert.gov/cas/techalerts/TA07-192A.html>

- 35. July 11, ComputerWorld — Israeli security firm reports huge spike in PDF spam.** Israeli security firm Commtouch Software Ltd. is warning of a massive surge in PDF spam. According to estimates by the company, about 10 percent to 15 percent of all spam over the past day or so has been in the form of PDF messages. "Given the fact that these messages are nearly four times bigger than standard spam messages, this increases overall global spam traffic by 30 percent to 40 percent," said Rebecca Herson, senior director of marketing at the Israel-based company. So far, the outbreak has involved 14 billion to 21 billion PDF unsolicited messages and shows no signs of slowing, Herson said. An analysis of the outbreak shows it to be a truly global zombie-distributed spam attack, Herson said. About 24 percent of the spam e-mails are from the U.S., 14 percent are from Taiwan, and China and Russia accounted for 10 percent and 4 percent, respectively. In all, PDF spam e-mails are being distributed by computers in 167 countries. According to Herson, the technique of sending messages as PDF attachments is relatively new and was first detected only a few weeks ago. The current outbreak shows that spammers have widely adopted the technique, she said.  
Source: [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026840&intsrc=hm\\_list](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026840&intsrc=hm_list)

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://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 <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983-3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> 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](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.