



# Department of Homeland Security Daily Open Source Infrastructure Report for 27 October 2006

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

- Computerworld reports that according to Javelin Strategy & Research, the problem of online identity theft is vastly hyped when compared with its more prevalent off-line equivalent, since more than 90 percent of identity fraud starts with stolen bank statements, misplaced passwords and such. (See item [8](#))
- The Associated Press reports President George W. Bush signed a bill on Thursday, October 26, authorizing 700 miles of new fencing along the United States–Mexico border, in an effort to secure the nation's borders and halt illegal immigration. (See item [11](#))
- The Harvard School of Public Health conducted a survey that found when faced with an outbreak of pandemic flu, a large majority of Americans would cooperate with public health officials' recommendations to curtail various activities of their daily lives, such as using public transportation, going to the mall, and going to church. (See item [22](#))

### 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. *October 26, Associated Press* — **Fire engulfs oil distributor's warehouse in Iowa.** A motor oil distributor's warehouse caught fire early Thursday, sending flames 30 feet into the air and

pumping thick black smoke over the surrounding fields. The 11,250–square–foot Stern Oil Co. building was engulfed in flames. It housed cases of motor oil, bulk oil and air filters, said company President Gillas Stern. He said no employees were injured but did not know what sparked the early morning fire.

Source: <http://msnbc.msn.com/id/15427630/>

2. *October 25, Independent Weekly (NC)* — **State regulators fault guard training at nuke plant.** A state probe into charges of cheating on certification exams by security staff at Progress Energy's Shearon Harris nuclear power plant found improper training of the plant's guards, who are responsible for protecting not only the facility's reactor but also one of the nation's largest stockpiles of highly radioactive spent fuel. The investigation by the North Carolina Private Protective Services Board (PPSB), a division of the state attorney general's office, found that handgun training for Harris guards was provided by instructors lacking proper certification and that guards were recertified without a required annual refresher course. It also questioned whether Harris guards have been getting adequate training in other critical areas, including legal search procedures and contraband detection. The PPSB is now reconsidering a 15–year–old agreement giving utility companies broad control over firearms training and reasserted its oversight at North Carolina's three nuclear power plants. An investigator assigned by PPSB found evidence of guards cheating on an annual written test required by the federal Nuclear Regulatory Commission (NRC). The NRC is wrapping up its own investigation into cheating and other security problems. The agency has confirmed some of the guards' complaints, including reports that security doors were left malfunctioning for long periods.

Source: <http://www.indyweek.com/gyrobase/Content?oid=oid%3A39253>

3. *October 25, Federal Energy Regulatory Commission* — **FERC institutes inquiries into gas–electric coordination issues.** The Federal Energy Regulatory Commission (FERC) is concerned that the scheduling practices of independent system operators (ISOs) and regional transmission organizations (RTOs) are not effectively coordinated with the scheduling of natural gas purchase and transportation transactions, so that gas–fired must–run generators may be unable to obtain gas during periods when gas transportation is constrained or gas prices are volatile. To address these issues, the Commission will institute inquiries pursuant to section 206 of the Federal Power Act to provide the parties in ISOs and RTOs with forums in which to examine whether scheduling and compensation mechanisms need to be revised to ensure that gas–fired generators can obtain gas when the gas–fired generation is necessary for reliability and that they are compensated appropriately when volatility in gas prices creates difficulty in recovering gas costs.

Source: <http://www.ferc.gov/whats-new/comm-meet/101906/E-4.pdf>

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

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

Nothing to report.

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

## **Defense Industrial Base Sector**

4. *November 01, National Defense* — **While more research is directed to irregular combat, war spending could deter advances in military weapons.** Not long ago, discussions about the future of defense technology were dominated by a conviction that innovations in science would continue to deliver uncontested military superiority for the U.S. military. That boundless optimism has been tempered dramatically during the past three years by the realization that a mighty high-tech force could be challenged by ragtag insurgents and suicide bombers. At military laboratories today, speed is the focus. Despite this, much new technology currently is in the works that aims at reshaping the future of the military. However, analysts now project that military research and development (R&D) is in for tough times. The thinking is that the cost of the wars in Iraq and Afghanistan will continue to drain funds from procurement, science and technology, among other things. Kei Koizumi, director of R&D budget and policy programs at the American Association for the Advancement of Science, says the Pentagon plans to curtail spending on applied research. Of most concern, he says, is that only a small portion of the R&D money would go to basic research. That should worry military scientists, he says, because basic research dollars are the seed money that will lead to ground-breaking technologies decades from now.

Source: <http://www.nationaldefensemagazine.org/issues/2006/November/Whilemorereseach.htm>

5. *October 25, GovExec* — **IG Report: Overhead reached 55 percent in some Iraq contracts.** Overhead and administrative costs on Iraq reconstruction projects have run as high as 55 percent of total spending and could be even higher with full accounting, according to data in a new inspector general report. In a review of 12 large reconstruction contracts awarded in early 2004 by an Army contracting office, the Special Inspector General for Iraq Reconstruction found that contractors charged the government from 11 percent to 55 percent for overhead and administration. The contracts, all for design-build projects in which a single contract covers both stages of construction, were to be issued using new administrative task orders to help managers see the balance of direct and indirect costs, minimize administrative expenses and better understand how extending contracts affects indirect expenses.

IG report: [http://www.govexec.com/pdfs/SIGIR\\_ATO\\_Audit.pdf](http://www.govexec.com/pdfs/SIGIR_ATO_Audit.pdf)

Source: [http://www.govexec.com/story\\_page.cfm?articleid=35346&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=35346&dcn=to%20daysnews)

6. *October 24, National Journal* — **Defense official: Changes necessary to meet 'net-centric' goals.** The defense community's prevailing "information is power" attitude must evolve into "a culture that embraces and leverages the power of information," a senior Department of Defense official told the Military Communications Conference on Tuesday, October 24. The "need to know" regime is changing to one that focuses on "the need to share," said John Grimes, assistant secretary of defense for networks and information integration. "We must be stewards of the information, not the owners." Connecting people with data leads to information, which leads to knowledge, he said. Attaining DoD's "network-centric goals" involves changing the way it does business and the way it acquires capabilities quicker and cheaper, based on commercial practices, Grimes said. "Some will impact your business models," he warned attendees, many of whom were from the private sector. The Pentagon "must stop buying individual, highly tailored proprietary systems," and turn instead to vendors that can provide solutions for use within and across the military, he said. Grimes, who is also DoD's chief information officer, said the military is shifting to a portfolio management concept,

emphasizing managed services and service-oriented architectures, he said. A year ago, the catchphrase was "information assurance," but today he said "it's all about data."

Source: [http://www.govexec.com/story\\_page.cfm?articleid=35335&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=35335&dcn=to%20daysnews)

[[Return to top](#)]

## **Banking and Finance Sector**

7. *October 25, Dow Jones* — **U.S. government says counterfeit dollars not serious problem to economy.** Only about one in 10,000 U.S. currency notes is likely to be counterfeit, despite a mostly overseas market for U.S. dollars and new technologies that make it easier to produce phony money, according to an interagency U.S. government report Wednesday, October 25. "Counterfeiting is not currently a serious problem for the U.S. economy as a whole," according to an interagency report to Congress by the Federal Reserve, the Department of the Treasury, and the U.S. Secret Service. Counterfeiting remains low largely because of diligent investigation and prosecution, deterrent currency design and effective public education, the report says. Meanwhile, counterfeiters have benefited from the growing availability and falling cost of computers, software, and inkjet printers that can more easily mimic genuine currency. While counterfeiting in general appears to be "quite small" in relative terms, the report lists countries that have had the biggest seizures of fake dollars. In fiscal 2005, Peru topped the list, followed by Sri Lanka, Hong Kong, the Philippines, Singapore, China, Chile, Bolivia, Mexico and Taiwan.

Source: <http://www.nasdaq.com/aspx/content/NewsStory.aspx?cpath=20061025%5cACQDJON200610251751DOWJONESDJONLINE001245.htm&>

8. *October 25, Computerworld* — **Online ID fraud is hyped; real problem is off-line.** The problem of online identity theft is vastly hyped when compared with its more prevalent off-line equivalent, according to Javelin Strategy & Research. While keylogging software, phishing e-mails that impersonate official bank messages, and hackers who break into customer databases may dominate headlines, more than 90 percent of identity fraud starts off conventionally, with stolen bank statements, misplaced passwords, or other similar means, according to Javelin. While scammers often use the Internet to access existing bank, phone or brokerage accounts or to create new ones using stolen details, in only one out of 10 of those incidents did the actual theft of the personal data take place through e-mail or the Web or somewhere else on the Internet, according to Javelin. Bank customers in the U.S. are not the most frequent targets of the most common form of online identity theft, phishing attacks. McAfee reports that more than half of all recent phishing attacks involved e-mails from a sender masquerading as VolksBank, a German bank, with another quarter targeting customers of U.K. bank Barclays PLC.

Source: [http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=data\\_control\\_and\\_ip&articleId=9004429&taxonomyId=144](http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=data_control_and_ip&articleId=9004429&taxonomyId=144)

9. *October 24, CNET News* — **Telephone banking system recognizes your voice.** A system by RSA Security designed to help fight telephone banking fraud adds voice as a way for automated telephone banking services to identify users. "As we are strengthening security for the Web channel, phone banking is effectively becoming the next big target," said Christopher Young of RSA. The system generates a risk score by looking at the voiceprint as well as other

parameters, such as the phone number and user behavior profiles, RSA said. Low-risk transactions proceed uninterrupted, while transactions with a high-risk score are verified with an additional layer of security, such as secret questions, it said. Current phone authentication techniques lack security, as they are typically conducted semi-manually, and are susceptible to social engineering attacks, RSA said. Crooks are learning to take advantage of that, it added. Source: [http://news.zdnet.com/2100-1009\\_22-6129174.html](http://news.zdnet.com/2100-1009_22-6129174.html)

[[Return to top](#)]

## **Transportation and Border Security Sector**

10. *October 26, Department of Homeland Security* — **DHS: majority of Visa Waiver countries meet security upgrade to e-Passports.** The Department of Homeland Security (DHS) announced on Thursday, October 26, that nearly all of the Visa Waiver Program (VWP) countries have met the requirement for issuing e-Passports. Working in close collaboration with the United States, 24 of the 27 VWP countries have met today's deadline, requiring all newly issued passports to contain a contactless chip with the passport holder's biographic information and a biometric identifier, such as a digital photograph of the holder. An e-Passport securely identifies the bearer, defends against identity theft, protects privacy and makes it difficult for individuals to cross borders using fraudulent documents. During the past two years, the U.S. government has collaborated with VWP countries to develop the technical standards and capability to ensure that the e Passports were operable with the readers at U.S. ports of entry. The United States continues to work with the three countries not yet issuing e Passports, Andorra, Brunei and Liechtenstein, to ensure that they meet the requirement as soon as possible. Travelers who wish to verify whether or not their passports meet the requirements and deadlines for VWP travelers, can find details at <http://www.dhs.gov/xtrvlsec/>  
Source: [http://www.dhs.gov/xnews/releases/pr\\_1161876358429.shtm](http://www.dhs.gov/xnews/releases/pr_1161876358429.shtm)
11. *October 26, Associated Press* — **President Bush approves 700-mile border fence.** President George W. Bush signed a bill on Thursday, October 26, authorizing 700 miles of new fencing along the United States-Mexico border, hoping to give Republican candidates a pre-election platform for asserting they're tough on illegal immigration. "Unfortunately the United States has not been in complete control of its borders for decades and therefore illegal immigration has been on the rise," Bush said at a signing ceremony. He called the fence bill "an important step in our nation's efforts to secure our borders." The measure Bush put into law offers no money for the fence project covering one-third of the 2,100-mile border. The cost is not known, although a homeland security spending measure the president signed earlier this month makes a \$1.2 billion down payment on the project. The money also can be used for access roads, vehicle barriers, lighting, high-tech equipment and other tools to secure the border. President Bush's speech: <http://www.whitehouse.gov/news/releases/2006/10/20061026.htm> 1  
Statement by Department of Homeland Security Secretary Michael Chertoff: [http://www.dhs.gov/xnews/releases/pr\\_1161895282064.shtm](http://www.dhs.gov/xnews/releases/pr_1161895282064.shtm)  
Fact Sheet: The Secure Fence Act of 2006: <http://www.whitehouse.gov/news/releases/2006/10/20061026-1.htm>  
Source: <http://www.baltimoresun.com/news/nationworld/bal-bush1026.0.4041390.story?coll=bal-nationworld-headlines>



12. *October 26, GovExec* — **Intelligence, homeland security agencies sharpen surveillance methods.** A senior Coast Guard official on Tuesday, October 24, praised homeland security and intelligence agencies' efforts to develop new surveillance tools and bolster information sharing. Guy Thomas, the Coast Guard's science and technology adviser, said improved surveillance techniques would help provide better protection against the possibility of attacks launched from boats offshore. For example, a 60- to 70-foot boat loaded with ordinary explosives and a biological or chemical weapon could deliver and spread a deadly substance — five pounds of anthrax, for example — to coastal areas with thousands of people, Thomas said at the Border Management Summit, which was organized by the Institute for Defense and Government Advancement. Protecting the coastal waters requires improved sensory techniques, said an official with a company that provides security solutions. He said his company has been working on multiple projects aimed at identifying incoming ships from farther away to detect suspicious ones. Recent advances mean that even the material from which a ship is built — whether it is wood, plastic or metal — can be determined from a distance.  
Source: [http://www.govexec.com/story\\_page.cfm?articleid=35330&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=35330&dcn=to%20daysnews)

13. *October 26, Northern Territory News (Australia)* — **Explosives stolen from train.** Counter-terrorism police are on the hunt for 400kg of the same type of explosive material used to kill 92 Australians in the two Bali bombings. The explosive grade ammonium nitrate was stolen from a freight train as it stopped to let another train pass at Glendale, near Newcastle NSW. The Daily Telegraph has learned NSW counter-terrorism police suspect a highly organized group used a crow bar to break special stainless steel seals on the carriage. The granular substance — it looks like grey gravel — was en-route to Kalgoorlie in Western Australia, where it was to be used by miners to blow through rock. Ammonium nitrate was the main ingredient used by the Bali bombers in both the 2002 and 2005 attacks, which left 225 people dead, including 92 Australians. NSW counter-terrorism police confirmed they were investigating the October 6 theft but declined to elaborate. The ammonium nitrate was owned by mining company Orica, which confirmed it was co-operating with NSW counter-terrorism police. Ammonium nitrate is a form of fertilizer that becomes a powerful explosive when mixed with common fuel oil. It is a favorite tool of terrorists and was used in the U.S.'s Oklahoma City bombing in 1996 and the World Trade Center bombing in 1993.  
Source: [http://www.ntnews.news.com.au/common/story\\_page/0.7034.20646 620%5E421.00.html](http://www.ntnews.news.com.au/common/story_page/0.7034.20646.620%5E421.00.html)

14. *October 25, GovExec* — **Arizona has tough fight ahead against illegal immigration.** For officials, times have been difficult along Arizona's 370-mile border with Mexico. Prosecutors are overwhelmed by immigration court cases. There were nearly 580,000 arrests of illegal immigrants in Arizona last year, and less than 170,000 spaces available to hold detainees at any given time. "We are now doing more public corruption cases than ever before," said Paul Charlton, U.S. Attorney for the District of Arizona. More bribes are being accepted, or at least more people are getting caught taking them, he said. In Yuma, where the bulk of Arizona's illegal border crossings occur, Border Patrol officials find themselves more often under siege from rocks and bullets than ever before, region Chief Patrol Agent Ronald Colburn said. Border Patrol officials even find their equipment under siege. Vandals routinely destroy cameras; to get past locked gates, smugglers carry blowtorches, Colburn said. Colburn said President Bush's decision to move National Guard troops to the Arizona border has been a relief for Border Patrol officials. He said about 118,000 illegal immigrants were caught in his section alone,

along with about \$36 million in drugs during the last fiscal year. Charlton said he would like to see penalties stiffened for illegal immigrant smugglers.

Source: [http://www.govexec.com/story\\_page.cfm?articleid=35350&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=35350&dcn=to%20daysnews)

15. *October 24, Department of Transportation* — **Public invited to comment on safety at private highway–rail grade crossings at San Francisco forum.** Continuing a national effort to improve safety and save lives at private highway–rail grade crossings, the Federal Railroad Administration (FRA) is holding a series of public meetings across the country, with the at San Francisco on Thursday, October 26. The purpose is to gather information to help FRA better understand the safety issues at locations where non–public roadways cross over railroad tracks used by freight and passenger trains. Approximately 400 vehicle–train collisions and 30 to 40 fatalities occur at the nation’s 94,000 private crossings each year. Since private crossings are not subject to the same federal rail safety regulations that public crossings are, FRA is seeking comments on several topics, including: how to define when a private crossing has a public purpose; how improvement and maintenance costs should be allocated; whether current warning devices for motorists are adequate; and if there should be a more uniform state or federal approach to improving safety at private crossings. Establishing responsibility for safety at private crossings is one of the primary goals of the U.S. Department of Transportation’s Highway–Rail Grade Crossing Safety and Trespass Prevention Action Plan issued in 2004. The public docket for review and consideration is available at <http://dms.dot.gov/> (FRA–2005–23281).

Source: <http://www.dot.gov/affairs/fra1606.htm>

[[Return to top](#)]

## **Postal and Shipping Sector**

16. *October 26, DM News* — **USPS ready for holidays.** The U.S. Postal Service (USPS) is prepared to handle an expected increase in volume this fall — most of it Standard Mail. The agency estimates that this year’s fall mailing season volume increase will be about four percent compared with the rest of the year, and about the same percentage as last year. The agency considers August 16 through the Wednesday before Thanksgiving its fall mailing season. Peak time for Standard Mail traditionally is the last week of October or first week of November, when the postal service delivers the most catalogs and ad mail. But now the USPS sees more ad mail later in November and even into December as consumers and companies realize that late orders still can be delivered in time for the holidays. Looking ahead to the holidays, Tony Pajunas, USPS vice president of network operations, said the peak mailing season begins November 24 and extends until December 31. “Every year at this time, we supplement our air networks by putting hundreds of trucks in place to really move the mail around the clock because the volume is so much higher than our normal volumes,” he said. The USPS also will increase the capacity that it buys from its air suppliers.

Source: <http://www.dmnews.com/cms/dm-news/direct-mail/38743.html>

17. *October 26, Naples Daily News (FL)* — **Bomb threat closes North Naples post office branch.** A bomb threat has forced the closure of a North Naples, FL, post office branch location. The Coco River branch received a bomb threat at 10:40 a.m. EDT by telephone. A caller said a bomb was in the building; employees were evacuated as officials called 911, post

office spokesperson Gary Sawtelle said. The Sheriff's Office bomb squad is investigating the incident, with assistance from the North Naples Fire Department. About 69 postal routes are served from the building, and mail from 41 of those routes remains inside.

Source: [http://www.naplesnews.com/news/2006/oct/26/bomb\\_threat\\_closes\\_north\\_naples\\_post\\_office\\_branch/?latest](http://www.naplesnews.com/news/2006/oct/26/bomb_threat_closes_north_naples_post_office_branch/?latest)

[[Return to top](#)]

## **Agriculture Sector**

18. *October 26, AFX News* — **Dutch authorities report three new cases of bluetongue disease in sheep.** Dutch authorities have reported three new cases of bluetongue disease, which is deadly to sheep, and enlarged the security zone around infected farms in the southern Netherlands. In total, 310 farms are now infected. There is already a large security zone set up in the southern Netherlands. Bluetongue is a non-contagious, insect-transmitted, viral disease of sheep, which is not known to affect humans. Other animals like cows and goats can carry the disease but will not get ill.

Bluetongue information: <http://www.fao.org/AG/AGAINFO/subjects/en/health/diseases-cards/bluetongue.html>

Source: [http://www.hemscott.com/news/latest-news/item.do?newsId=3701\\_4028279068](http://www.hemscott.com/news/latest-news/item.do?newsId=3701_4028279068)

19. *October 25, Dow Jones Newswires* — **Audit: USDA needs tighter oversight on bovine tuberculosis.** Federal officials at the U.S. Department of Agriculture (USDA) need to pay closer attention to state surveillance reports on bovine tuberculosis (TB) in order to achieve success in wiping out the a contagious cattle disease, according to an audit performed by USDA's Office of the Inspector General (OIG). OIG auditors said USDA's Animal and Plant Health Inspection Service (APHIS) "was not using its oversight tools timely or effectively" during a review conducted in 2004. State agriculture officials, OIG said, routinely document surveillance efforts for the disease, but "monthly reports were not being reviewed by the national or regional offices." APHIS Administrator Ron DeHaven, in an official response to the audit, pledged to set up new procedures to review state surveillance reports by the end of 2006.

Audit Report: <http://www.usda.gov/oig/webdocs/50601-09-CH.pdf>

Source: <http://www.cattlenetwork.com/content.asp?contentid=79043>

[[Return to top](#)]

## **Food Sector**

20. *October 25, Animal and Plant Health Inspection Service* — **USDA allows shelled garden peas from Kenya.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service today announced that it is amending its regulations to allow, under certain conditions, the importation of shelled garden peas from Kenya into the continental U.S. To be eligible for importation, the peas must be shelled and disinfected. They must also be inspected and accompanied by a phytosanitary certificate issued by the Kenya Plant Health Inspectorate. The certificate must include a declaration that the peas have been shelled, washed and found to be free of pests, such as the cotton bollworm.



Source: <http://www.aphis.usda.gov/newsroom/content/2006/10/kenyapeas.shtml>

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

## **Water Sector**

### **21. *October 24, Water Environment Federation* — Security training program receives funding.**

The Water Environment Federation (WEF) has been selected by the U.S. Department of Homeland Security to receive \$1.7 million to implement a three-year comprehensive training program addressing interdependencies between the water sector and other critical infrastructures. WEF will examine interdependencies within and outside the water sector in order to foster and enable effective partnerships that can advance prevention, protection, response, and recovery from incidents of national significance. The training will focus not just on water and wastewater (water sector) utilities but also on managers from other related critical infrastructures and on local government officials.

Source: [http://www.wef.org/CmsWEF/Pages/News/StoryPage.aspx?story\\_id=99486292&ID=wef&Section=Industry%20News](http://www.wef.org/CmsWEF/Pages/News/StoryPage.aspx?story_id=99486292&ID=wef&Section=Industry%20News)

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

## **Public Health Sector**

### **22. *October 26, Harvard School of Public Health* — In the case of an outbreak of pandemic flu Americans willing to make major changes in their lives.** A national survey conducted by the Harvard School of Public Health (HSPH) finds that when faced with an outbreak of pandemic flu, a large majority of Americans are willing to cooperate with public health officials' recommendations. More than three-fourths of Americans say they would cooperate if public health officials recommended that for one month they curtail various activities of their daily lives, such as using public transportation, going to the mall, and going to church. More than nine in ten say they would stay at home away from other people for seven to ten days if they had pandemic flu. In addition, 85 percent say they and all members of their household would stay at home for that period if another member of their household was sick. Nine in ten Americans say that if public health officials recommended that they and the other members of their household stay in their city, they were likely to stay. While 57 percent of employed adults say they would stay home from work if public officials said they should, even if their employers told them to come to work, about 35 percent say they would go to work.

Survey: [http://www.hsph.harvard.edu/panflu/panflu\\_release\\_topline.doc](http://www.hsph.harvard.edu/panflu/panflu_release_topline.doc)

Slides: [http://www.hsph.harvard.edu/panflu/panflu\\_charts.ppt](http://www.hsph.harvard.edu/panflu/panflu_charts.ppt)

Source: <http://www.hsph.harvard.edu/press/releases/press10262006.htm>

### **23. *October 26, Xinhua (China)* — Sparrows in China carry bird flu virus.** Chinese scientists recently reported that they found H5N1 bird flu virus in sparrows two years ago, the first time the virus has been detected in the common, non-migratory bird on the Chinese mainland. Wuhan Institute of Virology in central China's Hubei Province tested excrement samples from 38 sparrows after an outbreak of bird flu in a county in Henan Province in 2004. Some of samples tested positive of H5N1 virus, said Li Tianxian, a researcher with the institute.

Working with the Beijing Institute of Zoology, under the Chinese Academy of Sciences, the scientists isolated four H5N1 strains among the 25 positive excrement samples. Li said tests on the four strains have shown they are a new genotype of H5N1.

Source: [http://news.xinhuanet.com/english/2006-10/26/content\\_5253696.htm](http://news.xinhuanet.com/english/2006-10/26/content_5253696.htm)

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

## **Government Sector**

Nothing to report.

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

## **Emergency Services Sector**

**24. *October 26, Washington Post* — Road-user group gives failing grade to majority of urban areas.** Making a familiar case for more roads and using the newer argument of homeland security, a trade association for highway builders and the automotive industry recently gave most of the nation's biggest metropolitan areas failing grades for how well they would evacuate their populations in a disaster. It recommended national standards, better planning and more roads and car ownership. The federal government is pushing coastal states to do some of that. Outside hurricane country and high-threat cities such as New York and Washington, however, experts are hard-pressed to envision scenarios in which officials would want to evacuate an entire metropolitan area in 12 hours. George W. Foresman, DHS undersecretary for preparedness, agreed that the "one-size-fits-all" approach does not work for different populations, transportation networks and risks in each city. But he said the highway users study is a bit of a straw man, because evacuation plans encompass preparations that would be useful in all kinds of emergencies, such as providing shelter and housing, improving communications, distributing medicine and health care, or setting up public alert and warning systems. "We are not doing it at the expense of scenarios that have a higher probability of occurring," Foresman said.

Report: [http://www.highways.org/pdfs/evacuation\\_report\\_card2006.pdf](http://www.highways.org/pdfs/evacuation_report_card2006.pdf)

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/10/25/AR2006102501765.html>

**25. *October 25, North Gate News Online (CA)* — Oakland International Airport simulates air crash disaster.** The Oakland International Airport served as the site of a simulated catastrophic airplane accident Tuesday, October 24. Starting at 7 a.m. PDT, the volunteers and more than 20 agencies, from fire departments to paramedics, gathered to simulate a crash and rescue. The Federal Aviation Administration mandates that airports conduct these emergency exercises every three years to make sure that an airport's plan to coordinate response teams actually works. Once all emergency crews completed the drill, the participating agencies critiqued their work. In this initial review, exercise coordinators said they met all of their goals. Airport officials and observers were generally pleased with the coordination of the exercise. Deborah Ale Flint, who manages operations at Oakland Airport, said the communications systems between the various agencies worked well, and though they did not need to use it, emergency teams tested a backup interoperability system used to patch together communication systems

that cannot talk to one another. However, there were some glitches. Some emergency teams who arrived at the site after the initial wave of firefighters and paramedics said they had difficulty finding the command center when they arrived. Over the next few weeks, airport officials will review evaluations of the exercise.

Source: <http://journalism.berkeley.edu/ngno/stories/027750.html>

26. *October 25, Government Computer News* — **National Guard overcoming communication shortfalls.** The Department of Defense has responded to performance shortfalls during last year's hurricane season by upgrading and disseminating technology that promotes communications among responders. The National Guard Bureau also has invested in portal and collaboration tools which will facilitate planning and information sharing among the local, state and federal entities that respond to disasters and other domestic incidents, according to Maj. Gen. Alan Cowles, director of the command control, communications and computer systems division for the bureau. The National Guard Bureau is using supplemental congressional funding to upgrade its interim satellite incident site communications sets, which it deployed in 11 states, to field an upgraded version called the Joint Incident Site Communications Capability (JISCC). JISCC packages can be towed or airlifted to incident sites and can communicate via high-frequency radio, telephone, video and satellites to interface a variety of communications equipment used by first responders and state and federal agencies. "We are on track to have this rapid-response capability in all 54 states and territories by mid-2007," Cowles said.
- Source: [http://www.gcn.com/online/vol1\\_no1/42398-1.html](http://www.gcn.com/online/vol1_no1/42398-1.html)

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

## **Information Technology and Telecommunications Sector**

27. *October 25, Security Focus* — **Microsoft Internet Explorer 7 pop-up window address bar spoofing weakness.** Microsoft Internet Explorer 7 is prone to a weakness that allows attackers to spoof a pop-up window and address bar. Attackers may exploit this via a malicious Webpage to spoof the contents and origin of a page that the victim may trust. This vulnerability may be useful in phishing or other attacks that rely on content spoofing.
- Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.
- Source: <http://www.securityfocus.com/bid/20728/references>
28. *October 25, Security Focus* — **Toshiba Bluetooth Stack unspecified remote memory corruption vulnerability.** Toshiba Bluetooth Stack is prone to an unspecified remote memory corruption vulnerability. Successfully exploiting this issue allows remote attackers to execute arbitrary machine code in the context of the kernel running the affected software, facilitating the complete compromise of affected computers. Failed exploit attempts likely result in denial-of-service conditions. Versions 3 through 4.00.35 of the Toshiba Bluetooth stack are vulnerable to this issue. OEM vendors such as Dell, Sony, ASUS, and potentially others include vulnerable versions of the affected software.
- Solution: The vendor has released updates to address this issue. For more information on obtaining and applying fixes: <http://www.securityfocus.com/bid/20489/references>
- Source: <http://www.securityfocus.com/bid/20489/discuss>

29. *October 25, Security Focus* — **Cisco Security Agent remote port scan denial-of-service vulnerability.** Cisco Security Agent for Linux is vulnerable to a remote denial-of-service vulnerability. Analysis: The application fails to properly handle unexpected network traffic. Successfully exploiting this issue allows remote attackers to cause the affected software to enter into an unresponsive state, denying further service to legitimate users.  
For a complete list of vulnerable products: <http://www.securityfocus.com/bid/20737/info>  
Solution: Cisco has released an advisory and fixes to address this issue. For more information on obtaining and applying fixes: <http://www.securityfocus.com/bid/20737/references>  
Source: <http://www.securityfocus.com/bid/20737/discuss>
30. *October 25, eWeek* — **Study: Technology not an IT security solution.** Management support of security policies is the most important element in effectively securing organizations' infrastructure, according to the third annual Global Information Security Workforce Study, conducted by analyst firm IDC and sponsored by the (ISC)<sup>2</sup>. The list of imperative ingredients for a secure infrastructure also included having users follow security policy, having qualified security staff, and software and hardware solutions. Responses came from more than 4,000 information security professionals in over 100 countries. Technology as an enabler, but not the solution, for implementing a sound security strategy was an ongoing theme in the results. Processes and people were also highlighted in responses; these are areas which have been traditionally overlooked in favor of trusting hardware and software to solve security problems. The study, released Wednesday, October 25, found that increasingly, responsibility for security information assets is shifting from the chief information officer to other senior managers, and in many cases, outside IT altogether to chief financial and chief risk officers and legal and compliance departments.  
Global Information Security Workforce Study (registration required):  
[https://www.isc2.org/cgi-bin/request\\_wfstudy\\_public.cgi](https://www.isc2.org/cgi-bin/request_wfstudy_public.cgi)  
Source: <http://www.eweek.com/article2/0.1759.2037326.00.asp>
31. *October 25, CNET News* — **Citywide Wi-Fi spending could hit \$3 billion.** More than \$3 billion will be spent during the next four years to build and operate public wireless networks for U.S. municipalities, according to a new research report by MuniWireless.com. Interest among U.S. cities and counties to deploy their own public wireless networks is exceeding earlier expectations, said Esme Vos, founder of MuniWireless.com, which tracks the muni-wireless market. Citywide Wi-Fi networks, which are built and managed by a city alone or in partnership with a private company, have come into vogue in the past couple of years. With these new networks, is a promise to provide affordable or free broadband access to residents. But the technology is not without challenges, as cities such as Tempe, AZ, have discovered. Because Wi-Fi uses unlicensed spectrum, interference from other wireless devices can be a problem. Coverage can also be an issue, since signals often don't reach inside homes without special devices to boost the signal indoors.  
Source: [http://news.com.com/Citywide+Wi-Fi+spending+could+hit+3+billion/2100-7351\\_3-6129655.html?tag=nefd.top](http://news.com.com/Citywide+Wi-Fi+spending+could+hit+3+billion/2100-7351_3-6129655.html?tag=nefd.top)
32. *October 25, VNUNet* — **Microsoft opens up anti-spam standard.** Microsoft has released its Sender ID Framework specification under the company's Open Specification Promise. This allows software developers and service providers to use the technology without having to pay a license fee to Microsoft. In the past Sender ID has drawn fire from open source developers

because the previous Microsoft license didn't allow the technology to be deployed in combination with open source software.

Source: <http://www.vnunet.com/vnunet/news/2167188/microsoft-opens-an-ti-spam>

## Internet Alert Dashboard

Current Port Attacks	
<b>Top 10 Target Ports</b>	15281 (----), 37384 (----), 6346 (gnutella-svc), 4662 (eDonkey2000), 11266 (----), 6881 (bittorrent), 1026 (win-rpc), 2234 (directplay), 65530 (WindowsMite), 51344 (----)
Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center	
To report cyber infrastructure incidents or to request information, please contact US-CERT at <a href="mailto:soc@us-cert.gov">soc@us-cert.gov</a> or visit their Website: <a href="http://www.us-cert.gov">www.us-cert.gov</a> .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <a href="https://www.it-isac.org/">https://www.it-isac.org/</a> .	

[[Return to top](#)]

## Commercial Facilities/Real Estate, Monument & Icons Sector

33. *October 26, Statesman Journal (OR)* — **Man ignites fires inside crowded Oregon church.** A man entered the Peoples Church on Lancaster Drive during a Wednesday evening, October 25, worship service packed with several hundred people and used a burning liquid to set fires in the crowded sanctuary, officials and witnesses said. One woman, identified by a church pastor as Arlene Anderson, reportedly was taken to the hospital by her husband for medical attention to burns on her back and neck. Witnesses said the liquid, possibly gasoline, was igniting as it came out of a can that the man was holding. It was not clear how the man ignited the liquid. Deputy Kevin Rau, a spokesperson for the Marion County Sheriff's Office, said one man was in custody. Rau said the man arrived at the church in a taxicab and threatened the cab driver with a knife. Rau said the Salem-Keizer Yellow cab driver and the man wrestled for the knife. During the struggle, the cab driver suffered a minor injury to his neck. Miller said church members tackled the man and were able to get him out of the church. Other churchgoers were able to put out the flames using fire extinguishers or by beating down the flames with clothing.
- Source: [http://159.54.226.83/apps/pbcs.dll/article?AID=/20061026/NEW\\_S/610260329](http://159.54.226.83/apps/pbcs.dll/article?AID=/20061026/NEW_S/610260329)

34. *October 26, Times-Picayune (LA)* — **New report disputes corps-led levee probe.** A hard-hitting review by an elite science and engineering panel has prompted the investigation team led by Army Corps of Engineers to recant parts of its investigation into levee failures during Hurricane Katrina, including statements in a draft report released five months ago purporting that there was no evidence of negligence or malfeasance by the corps or its contractors. The panel's report also takes issue with the original draft's contention that the major cause of the failures could not have been foreseen by the levee system's designers, a finding the corps has not removed from its original report. One of the leaders of the corps-led Interagency Performance Evaluation Task Force, or IPET, whose 150 members come from academia, private industry and the corps, said his team is not disputing most the findings of the review, done by a committee of the National Academy of Engineers and the National Review Council of the National Academies University of Maryland senior search engineer Ed Link, who shares



leadership of the IPET project with two corps representatives, said the group was under "severe time pressures to get a decent final draft out by June 1.

Source: [http://www.nola.com/frontpage/t-p/index.ssf?/base/news-6/116\\_1842104280850.xml](http://www.nola.com/frontpage/t-p/index.ssf?/base/news-6/116_1842104280850.xml)

**35. *October 26, Los Angeles Times* — Officials seek arsonist responsible for Southern**

**California fire.** Four firefighters were killed and another critically burned Thursday, October 26, trying to protect homes from a wind-whipped arson fire that charred more than 10,000 acres and forced hundreds to flee several mountain communities west of Palm Springs in Southern California. Authorities said the fire was set shortly after 1 a.m. southeast of Cabazon. The mountain blaze, known as the Esperanza Fire, forced 500 residents to evacuate from the remote communities of Twin Pines, Poppet Flat and Silent Valley. Hundreds of homes were threatened. Several hundred people in the Silent Valley recreational vehicle park were surrounded by fire after flames blocked their exit. Firefighters circled the park to keep the flames at bay. About 1,000 firefighters battled the blaze, but access was limited due to the steep, rugged terrain in the foothills of the San Jacinto Mountains. Officials said the fire could burn thousands more acres if it reaches parts of the San Bernardino National Forest where an infestation of pine bark beetles have left stands of dead trees. Riverside County Supervisors offered a \$100,000 reward leading to the arrest and conviction of the arsonist.

Source: <http://www.latimes.com/news/local/la-102606fire.0,1086207.story?coll=la-home-headlines>

[[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](mailto: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](mailto: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](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.