



Department of Homeland Security Daily Open Source Infrastructure Report for 04 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

- The National Governors Association Center for Best Practices is launching a major effort to help states prepare for all aspects of a potential influenza pandemic with the Pandemic Preparedness Project that addresses the issues of public health preparedness, government planning, maintenance of essential services, and community-based response strategies. (See item [27](#))
- The New York Times reports schools around the country are on alert with some school administrators and security experts worried about a new pattern of violence for which schools are not well prepared: adults with grudges or suicidal urges entering schools to inflict violence on students. (See item [29](#))
- The Detroit News reports undercover Detroit officers have arrested three suspects in the theft of about \$400,000 in copper from two municipal facilities. (See item [37](#))

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 02, Canadian Press* — **Report on massive 2003 blackout finds significant progress has been made.** Significant progress has been made on all 46 recommendations submitted to

Canadian and American officials in the wake of the blackout of 2003, according to the final report on the massive power outage. The report, released Monday, October 2, by the U.S.–Canada Power System Outage Task Force, says much has been accomplished in the three years since the blackout, which knocked out power for 50 million people on August 14, 2003. The report says no one can guarantee there won't be another big blackout, but new rules and reliability standards should result in a stable electricity supply on both sides of the border. Improved collaboration has resulted in 102 new standards being submitted to Canadian and American authorities for review and approval, and more are being developed, the report states. Still, the report concludes that governments can't be complacent, the causes of the blackout were traced to failures to comply with voluntary measures and mistakes that were repeated from previous blackouts.

Blackout report: http://www2.nrcan.gc.ca/es/erb/erb/english/View.asp?x=690&oi_d=1221

Source: <http://www.canada.com/topics/news/national/story.html?id=d86272c7-5361-4ff9-8743-0cd7f3b009d9&k=32181>

2. *October 02, Austin American–Statesman (TX)* — **Security lacking in networks controlling nuclear power stations, electrical grids, water lines.** Supervisory Control and Data Acquisition (SCADA) networks control nuclear power stations, water and gas lines, chemical plants, and other critical infrastructure. Many of them could be just as vulnerable today to attacks from computer hackers — or terrorists — as the Soviet system was nearly 25 years ago. Or even more vulnerable. That's because today, machines and computers are increasingly connected in a haphazard way to the Web. Rapid growth in easy-to-access wireless networks and the use of off-the-shelf software from Microsoft Corp. and others have also contributed. Hence the fear that five years after September 11, SCADA networks could become "the new airplanes," said Alan Paller of the SANS Institute. SCADA computers monitor and control the flow of electricity across the nation's power grids. Despite its importance, SCADA security is often an afterthought for corporate cybersecurity departments. That's because, so far, the networks haven't attracted computer hackers like financially oriented e-mail and online billing systems and corporate Websites have. "It's kind of like out of sight, out of mind," said Brian Davison of Austin Energy. At many utilities, "management has been away from the table," Davison said.
Source: <http://www.statesman.com/news/content/news/stories/nation/10/02/2scada.html>

3. *October 02, Reuters* — **Nuclear Regulatory Commission to investigate Arizona nuclear plant.** The U.S. Nuclear Regulatory Commission (NRC) said it would start on Tuesday, October 3, a special inspection of the United States' biggest nuclear plant, Palo Verde, in Arizona, after the recent failure of an emergency backup generator. In mandatory monthly checks, the emergency diesel generator failed during July 25 and September 22 tests at Unit 3 of the three-unit power station. For the Palo Verde nuclear power plant this is the latest in a string of setbacks. Arizona Public Service (APS), the station's operator, has for most of the last year had at least one of its three nuclear reactors out of service for unplanned maintenance. The generators are supposed to be available to produce electricity for safety systems at Palo Verde in case off-site power is lost, the NRC said. The NRC will "evaluate the adequacy of the licensee's response to the situation, the root cause of the problem, corrective actions, and determine if there are generic implications for other nuclear power plants." The NRC will issue a report in approximately one month that will be posted on the NRC's Website, <http://www.nrc.gov>.

NERC press release: <http://www.nrc.gov/reading-rm/doc-collections/news/2006/06-022iv.html>

Source: http://today.reuters.com/news/articleinvesting.aspx?view=CN&storyID=2006-10-03T042143Z_01_N02415580_RTRIDST_0_UTILITIES-PINNACLEWEST-APS.XML&rpc=66&type=qcna

4. *October 02, U.S. Department of Energy* — **Department of Energy releases strategic plan to address energy challenges.** Secretary of Energy Samuel W. Bodman Monday, October 2, released the Department's five-year strategic plan that focuses on the Department's role in powering and securing America's future. The plan addresses overall Department goals for developing and deploying new clean energy technologies, reducing our dependence on foreign energy sources, protecting our nuclear weapons stockpile, and ensuring that America remains competitive in the global marketplace. The Department's plan builds on President Bush's Advanced Energy and American Competitiveness Initiatives, which are increasing America's energy security, spurring scientific innovation, and sustaining our economic vitality. The Department's strategic plan seeks to deliver results along five strategic themes that include promoting America's energy security through reliable, clean, and affordable sources; ensuring America's nuclear security by transforming the nuclear weapons stockpile through development of Reliable Replacement Warheads that are safer and more secure; strengthening U.S. scientific discovery, economic competitiveness, and improving quality of life through scientific innovations; protecting the environment through responsible resolution of weapons era waste; and strengthening the operations and management of the Department. 2006 Strategic Plan: <http://www.energy.gov/about/strategicplan.htm>. Source: <http://www.energy.gov/news/4279.htm>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[[Return to top](#)]

Defense Industrial Base Sector

5. *October 02, Government Computer News* — **Department of Defense budget authorized.** House and Senate conferees have authorized the Department of Defense to spend \$532.8 billion on its programs in fiscal 2007. The full House and Senate passed the conference report Friday, September 29; now the bill will be sent to President Bush to be signed into law. The report includes \$84.2 billion in procurement funding; \$73.6 billion for research, development, testing and evaluation; \$110.1 billion for military personnel; and \$115.3 billion for operations and maintenance. Source: http://www.gcn.com/online/vol1_no1/42159-1.html
6. *October 02, Associated Press* — **Department of Defense must speed up procurement process.** As the U.S. continues to fight the Global War on Terror at home and abroad, the Department of Defense needs to change its procurement processes to put leading-edge

technology in war fighters' hands, a top Pentagon official said Monday, October 2. "There's nothing rapid about the procurement process ... right now," said Navy Vice Adm. Nancy Brown, adding that inefficient management of the military's frequency spectrum used for various communications systems is "putting war fighters in jeopardy. Our whole focus needs to change," said Brown, director of command, control, communications and computer systems for the Joint Staff and principal adviser to Gen. Peter Pace, Chairman of the Joint Chiefs of Staff. The Pentagon is attempting to increase both information sharing and security across military and civilian agencies toward the goal of providing the right data anywhere at anytime in an effort it calls "joint, net-centric operations." But managing the network is a gargantuan challenge when the various stake holders have different missions, buying strategies and levels of bureaucracy. One military service may upgrade its servers and if another does not, an outage can occur "and that hurts the warfighter," Brown said.

Source: <http://www.chron.com/disp/story.mpl/ap/fn/4230727.html>

[[Return to top](#)]

Banking and Finance Sector

7. *October 02, Associated Press* — **Protesters throw explosives at banks in southern Mexican city.** Mexico protesters threw explosives at two banks in Oaxaca on Monday, October 2, shattering windows and further raising tensions. The attacks on the banks by the previously unknown group called the Armed Revolutionary Organization for the People of Oaxaca follow months of violence in Oaxaca city, where protesters have set up street barricades and taken the city center. The explosions damaged the banks' facades, but caused little other damage, city official Eliodoro Diaz said. Protesters and news media speculated that federal forces were planning to retake the city after navy helicopters flew over the area this weekend. Interior Secretary Carlos Abascal insisted the helicopters and military planes were on routine supply runs that had nothing to do with the more than four months of unrest. The unrest began in May, when tens of thousands of teachers seized the capital's central plaza to demand wage increases. The following month, Governor Ulises Ruiz sent police to attempt to retake the heart of the city. Since then, thousands of leftists, students and anarchists, have joined striking teachers, building street barricades, burning buses and taking over radio and television stations.
Source: http://www.iht.com/articles/ap/2006/10/02/america/LA_GEN_Mexico_Oaxaca_Unrest.php

8. *October 02, CNET News* — **Court puts stop on online check firm.** A federal judge has ordered online payment processor Qchex to cease its current method of online payment processing, which U.S. regulators say facilitated fraud. Qchex let people create and send checks drawn on any bank account without verifying their authority to do so, the Federal Trade Commission (FTC) said Monday, October 2. The business focused on generating electronic checks online that could be e-mailed and then printed out by the recipient. "As a result, con artists have used the Qchex service to draw checks on bank accounts that belong to others," the FTC said, adding that it has received hundreds of consumer complaints about the company. Scammers used Qchex to pay individuals or businesses for goods or services. The checks would initially clear, but ultimately be canceled by the legitimate account holder. By then, the goods or services would have already been delivered, leaving the seller with a loss, the FTC said.
Source: <http://news.com.com/Court+puts+stop+on+online+check+firm/210>

9. *October 02, Websense Security Labs* — **Multiple Phishing Alert: Brazilian Gol Airlines Crash, National Bank of Abu Dhabi, Arkansas Federal Credit Union.** Websense Security Labs has received reports of a fraudulent e-mail which targets Brazilian users. Users receive an e-mail with a link to a malicious Website containing pictures of the recent Gol Airlines Boeing 737 crash in Brazil. This website contains a Trojan downloader which is used to install a banking keylogger. Another phishing attack targets customers of National Bank of Abu Dhabi. Users receive a spoofed e-mail message, which claims that multiple login attempts from blacklisted IPs have been detected and for this reason the account has been suspended. Users are asked to verify their login details by going through an extra verification process. The e-mail provides a link to a phishing site that attempts to collect user account information. Another attack targets customers of Arkansas Federal Credit Union. Users receive a spoofed e-mail message, which claims that an error has been detected in their billing information and details must be confirmed. The e-mail provides a link to a phishing site that attempts to collect user account information.

Screenshots: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=646>

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=645>

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=643>

Source: <http://www.websense.com/>

[[Return to top](#)]

Transportation and Border Security Sector

10. *October 03, New York Times* — **Cockpit recorders found in Amazon wreckage.** Rescue workers on Monday, October 2, found cockpit voice and data recorders near the wreckage of a Boeing 737, operated by the Brazilian carrier Gol Linhas Aéreas Inteligentes, which crashed in the Amazon rain forest Friday, September 29, killing all 155 people on board. Investigators continued questioning the American pilots of an Embraer Legacy 600 executive jet that the Brazilian authorities say they believe may have collided with the larger aircraft in midair. A senior executive of ExcelAire Service, a New York-based aircraft charter and management company that had purchased the smaller jet in Brazil and was taking it back to the United States, was also being questioned. Brazilian officials said that they expected the salvage and cleanup efforts at the crash site to take weeks, and that they had invited investigators from the United States National Transportation Safety Board to help.

Source: http://www.nytimes.com/2006/10/03/world/americas/03crash.html?_r=1&oref=slogin

11. *October 03, CNN* — **Jet hijack to protest pope's visit.** A Turkish airplane carrying 113 people was hijacked Tuesday, October 3, by two Turks protesting Pope Benedict XVI's upcoming visit to Turkey. The plane landed safely in Italy, according to a Turkish national airline official. The plane departed Tirana, Albania, and was headed to Istanbul, Turkey, when the hijackers announced their intentions over Greek airspace, the spokesperson said on Turkish television. The plane sent out an SOS signal and Greek defense ministry planes escorted the aircraft out of Greek airspace. Greek officials alerted their Italian counterparts, the spokesperson said. The plane, carrying 107 passengers and six crew, landed at a military airport in Brindisi, on the heel of Italy's boot.

Source: <http://www.cnn.com/2006/WORLD/europe/10/03/turkey.hijack/index.html>

12. *October 03, Associated Press* — Amtrak installing chemical sensors at Union Station.

Amtrak plans to install a sensor system meant to detect a possible chemical or poison gas attack at Washington, DC's Union Station. Amtrak spokesperson Karina Romero says the railroad would also install the sniffers in its section of Penn Station and at stations in Chicago and Philadelphia. The sensors, which are housed in simple metal boxes, are known as Protect. The system, which continually sucks in air and analyzes it for toxins and gases, was developed after the sarin gas attack in the Tokyo subway in 1995.

Source: http://www.wusatv9.com/news/news_article.aspx?storyid=52502

13. *October 02, Dallas Business Journal* — Wright bill passes. A bill that promises to lift Wright restrictions on Dallas' Love Field Airport was approved by Congress Friday, September 29. The bill, which has become known as the Wright compromise bill, provides immediate through-ticketing from Love Field Airport to anywhere in the country, as long as passengers first stop in one of the nine states where flights from Love Field are allowed under the Wright Amendment. In 2014, the 1979 federal law will be completely repealed. The bill also reduces gates at Love Field to 20 from 32. The passage of the bill will ultimately repeal the restriction the 1979 federal amendment placed on Love Field. Under the restrictions, flights from Love Field were limited to short-haul trips within Texas and to eight surrounding states. The bill, based on a local compromise agreement forged by the cities of Dallas and Fort Worth, American Airlines and the D/FW Airport board, was hard-fought. President Bush is expected to sign the bill as early as this week.

Source: <http://biz.yahoo.com/bizj/061002/1354477.html?.v=1>

14. *October 02, Toronto Sun (Canada)* — Quebec bridge collapse probe called. Using cranes and heavy machinery rescue workers painstakingly broke up concrete slabs Sunday evening, October 1, to free the bodies of five people killed when a section of an overpass collapsed on Saturday afternoon. The two vehicles removed from the rubble were crushed so badly they barely reached the knees of a firefighter at the scene. Only three of the five people killed, family members traveling together, were identified. The driver, Jean-Pierre Hamel, 40, his wife, Sylvie Beaudet, 44, and his brother, Gilles Hamel, 44, were on their way to visiting family in Montreal when the unthinkable happened. Six others were injured, two of them critically. Quebec Premier Jean Charest toured the site and announced a public inquiry into the collapse, which he described as "inexplicable." An inspector was sent to the overpass about half an hour before the tragedy on Saturday, after emergency calls reported chunks of concrete falling from the structure. Transport Minister Michel Despres said the inspector found no reason to close the overpass. "If there was the slightest indication that the bridge could fall, it would have been closed," Despres said.

Source: <http://www.torontosun.com/News/Canada/2006/10/02/1935513-sun.html>

[[Return to top](#)]

Postal and Shipping Sector

15. *October 03, Associated Press* — Postal testing increasing five years after anthrax deaths.

More than 1,000 biological detectors are sniffing mail across the country for dangerous contamination as the hunt goes on for whoever put anthrax in letters and killed five people just after the September 11 attacks. An anthrax case in Florida, reported five years ago Wednesday, October 4, brought the first hint of what turned out to be contamination of mail that reached Washington, New York, Connecticut, and New Jersey and raised fears nationwide. The Postal Service has taken action in an effort to prevent a repeat. "We have fully deployed the fleet of bio-detection systems" at 271 mail processing locations, Postal Vice President Tom Day said. Installation of the current system cost \$800 million, provided by Congress, and the post office is spending about \$70 million to operate it. That annual cost is expected to climb to \$120 million. The detectors check for anthrax and two other biological hazards. Day said workers now are trained to look for suspicious packages and call in postal inspectors if they detect something unusual. Among the things that make a package suspicious are leaking powder and liquids. In addition, there are other telltale signs that the agency does not like to discuss for fear of tipping off terrorists.

Source: <http://www.newsday.com/news/local/wire/connecticut/ny-bc-ct--afteranthrax1003oct03.0.5505197.story?coll=ny-region-apconnecticut>

[[Return to top](#)]

Agriculture Sector

16. *October 03, Agricultural Research Service* — **Cattle protozoa help shift antibiotic resistance.** Agricultural Research Service (ARS) scientists have made another big finding about protozoa found in the gastrointestinal tract of cattle. They've discovered that the protozoa can facilitate the transfer of antibiotic resistance from resistant bacteria to susceptible types. Veterinary medical officer Steven Carlson is the first scientist to document the role rumen protozoa play in transferring this resistance within cattle. Rumen protozoa live in the first stomach (rumen) of cattle. They engulf and destroy most bacteria. But Carlson and colleagues have identified and described the transfer of resistance to ceftriaxone, an antibiotic used to treat pneumonia, from gastrointestinal tract bacteria known as *Klebsiella* to rumen-dwelling *Salmonella* that are sensitive to the antibiotic. Carlson teamed with microbiologist Mark Rasmussen in a study that revealed for the first time that disease-causing bacteria can strengthen from interaction with protozoa that are naturally inside animals. In that work, an antibiotic-resistant strain of *Salmonella* became especially virulent when tucked within rumen protozoa. That discovery suggests that naturally occurring digestive tract protozoa may be a place where dangerous bacteria can lurk and develop.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

17. *October 02, Agence France-Presse* — **Netherlands erects fourth security zone to fight bluetongue disease.** Dutch officials have erected a fourth security zone around the eastern village of Bargem after the discovery of another case of bluetongue virus in sheep, the agriculture ministry has said. Three other security perimeters of 12 miles each are currently in place in the southern provinces of Brabant and Limburg, along the Belgian border. Exporting sheep outside these limits is strictly forbidden, and the animals must be enclosed at night. Bluetongue has been discovered in around 100 Dutch farms since mid-August.

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

Source: http://news.yahoo.com/s/afp/20061002/hl_afp/netherlandsagriculture_061002170711;_ylt=AuUy0MvHH.OODpYPato3XMCJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

18. *October 02, Animal and Plant Health Inspection Service* — **Final rule to regulate pine shoot beetle host material from Canada adopted.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is adopting as a final rule — with one change — an interim rule amending pine shoot beetle regulations concerning the importation of host material into the U.S. from Canada. This rule harmonizes U.S. regulations for trade in these host materials with regulations already in place in Canada. Under this rule, pine nursery stock, as well as pine products that consist of pine bark or have pine bark attached, must meet certain requirements regarding documentation, treatment, handling and utilization before they can enter the U.S. A written permit is required for the importation of all restricted pine articles, except seed. APHIS is, however, removing the import permit requirement for nonpropagative materials that are accompanied by a phytosanitary certificate or a certificate of movement and origin. This action is necessary to help prevent the introduction and spread of the pine shoot beetle into noninfested areas of the U.S. The pine shoot beetle currently infests portions of the northeastern U.S. The pine shoot beetle is a vector of several pine tree diseases that can cause economic losses to timber, Christmas tree and nursery industries.
Source: <http://www.aphis.usda.gov/newsroom/content/2006/10/psbcanada.shtml>
19. *October 02, National Science Foundation* — **New projects to get at the root of how genes control plant growth.** The National Science Foundation (NSF) made 24 new awards totaling \$72.5 million in the ninth year of its Plant Genome Research Program (PGRP). The two-to-five-year awards — ranging from \$600,000 to \$6.6 million — support research and tools to further knowledge about the genomes of economically important crop plants such as potato, poplar and corn, and will also reveal how networks of genes control basic plant processes. The new awards, made to 43 institutions in 30 states, include 10 international collaborations.
PGRP awards: <http://www.nsf.gov/bio/pubs/awards/pgr.htm>.
Source: http://www.nsf.gov/news/news_summ.jsp?cntn_id=108043&org=NSF&from=news
20. *September 29, Animal and Plant Health Inspection Service* — **Implementation of spring viremia of carp regulations delayed.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is delaying implementation of an interim rule published August 30 that restricts the importation into the U.S. of live fish, fertilized eggs and gametes of fish species that are susceptible to spring viremia of carp (SVC), a serious contagious viral disease of carp. The interim rule, Spring Viremia of Carp; Import Restrictions on Certain Live Fish, Fertilized Eggs and Gametes, was scheduled to take effect September 29. The implementation of the rule will be delayed 30 days to October 30. APHIS took this action to ensure that importers and foreign exporters have enough time to meet requirements of the rule. Under the interim rule, importers of SVC-susceptible species must obtain an import permit and a health certificate from the shipment's region of origin certifying that the live fish, fertilized eggs or gametes originated in an SVC-free area. This certification must be supported by ongoing SVC surveillance conducted under specific conditions for two years. In addition, live fish, fertilized eggs and gametes of SVC-susceptible species will be subject to additional new restrictions such as importation through designated ports of entry and meeting containment

requirements for shipments that are in transit through the U.S.

Source: <http://www.aphis.usda.gov/newsroom/content/2006/09/svcdelay.shtml>

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

Food Sector

21. *October 02, Associated Press* — **Two deaths in Georgia prompt raw oyster warning.** Raw oysters linked to the deaths of two Chatham, GA, women are believed to have come from the Gulf of Mexico, officials said. The source is still being investigated, said Coastal District Health Director Doug Skelton. But knowing the source may not help authorities prevent others from becoming infected, he said. He said the oysters were purchased from a restaurant and a retailer in the Savannah area. Skelton and Georgia Agriculture Commissioner Tommy Irvin warned consumers about eating raw oysters after the deaths of the two women, whose names were not released. The deaths are believed to have been caused by *Vibrio vulnificus*, a naturally occurring marine microorganism. On average, only 35 people contract the infection from shellfish annually in the U.S. The bacteria is associated with oysters raised in the Gulf of Mexico — the source of most raw oysters consumed in the U.S. — and other warm waters. Source: <http://www.news4jax.com/news4georgia/9983252/detail.html>

22. *October 02, AgProfessional* — **Carolina Turkeys buys Butterball Turkey.** Carolina Turkeys, an international turkey processing company headquartered in Mt. Olive, NC, Monday, October 2, announced that it has finalized the purchase of Butterball Turkey from ConAgra Foods, Inc. for \$325 million. The acquisition of Butterball, the most widely recognized brand in the turkey industry, immediately repositions Carolina Turkeys as the largest turkey producer in the U.S. The expanded company expects production to reach 1.4 billion pounds in 2006, or 20 percent of total turkey production in the U.S. Carolina Turkeys' company name has changed to Butterball LLC. For most of its 20-year history, Carolina Turkeys has been primarily a commodity business, selling whole birds and turkey products to grocery retailers and food service operators throughout the U.S. and in 15 countries around the world. In addition to the Butterball brand, Carolina Turkeys has acquired more than 3,200 employees and five processing plants in Huntsville, Ozark and Jonesboro, AR; Carthage, MO; and Longmont, CO. Source: http://www.agprofessional.com/show_story.php?id=43466

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

Water Sector

23. *September 29, Water Week* — **Utilities exempted from chemical security rules.** Under terms of a congressional deal, water and wastewater utilities will be exempted from interim chemical security requirements authorized in the FY 2007 spending bill for the Department of Homeland Security (DHS). The exemption gets water utilities using hazardous chemicals such as chlorine gas off the regulatory hook for having to repeat vulnerability assessments and emergency response planning previously mandated by the 2002 Bioterrorism Act. The exemption also applies to wastewater systems, which were not covered by the Bioterrorism Act but generally have voluntarily completed comparable assessments and plans with U.S. Environmental

Protection Agency assistance.

Source: <http://www.awwa.org/Communications/news/>

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

Public Health Sector

24. *October 03, PLoS Medicine* — A comparative analysis of influenza vaccination programs.

The threat of avian influenza and the 2004–2005 influenza vaccine supply shortage in the U.S. have sparked a debate about optimal vaccination strategies to reduce the burden of morbidity and mortality caused by the influenza virus. A recent study conducted by mathematical biologists at The University of Texas at Austin presents a comparative analysis of two classes of suggested vaccination strategies: mortality–based strategies that target high–risk populations and morbidity–based strategies that target high–prevalence populations. The study found that the optimal strategy depends critically on the viral transmission level of the virus: morbidity–based strategies outperform mortality–based strategies for moderately transmissible strains, while the reverse is true for highly transmissible strains. Furthermore, the study shows that vaccination delays and multiple introductions of disease into the community have a more detrimental impact on morbidity–based strategies than mortality–based strategies. The study concluded that if public health officials have reasonable estimates of the viral transmission rate and the frequency of new introductions into the community prior to an outbreak, then these methods can guide the design of optimal vaccination priorities. When such information is unreliable or not available, as is often the case, this study recommends mortality–based vaccination priorities.

Source: http://medicine.plosjournals.org/archive/1549–1676/3/10/pdf/10.1371_journal.pmed.0030387–S.pdf

25. *October 02, Scientific American* — Tuberculosis strain subverts immune response.

Researchers may have discovered the means by which the tuberculosis bacterium could adapt itself to different human populations. The loss of a gene from one strain of tuberculosis allows the bug to subvert the immune response of its host, potentially explaining why the strain caused an unusually severe outbreak at a UK school, researchers report. Related strains are a major cause of the disease in India and among Asians living in the UK, raising the possibility that the mutation could be part of an adaptation to those populations. The study found that the outbreak strain, which lacked a gene called Rv1519, grew at a normal pace in cultured human white blood cells, apparently by subverting the immune response to its benefit. The infected cells produce less inflammation–inducing chemicals — a major component of the immune response — and more anti–inflammatory chemicals.

Tuberculosis information: <http://www.cdc.gov/nchstp/tb/default.htm>

Source: <http://www.sciam.com/article.cfm?chanID=sa003&articleID=0007C452–7C20–1521–BB3483414B7F00FF>

26. *October 02, Infection Control Today* — Study demonstrates benefits of universal surveillance for MRSA and reveals need for repeated testing. A new study shows that implementing universal surveillance, which introduces the testing of all admitted patients, is far more effective than just passive or targeted active surveillance when monitoring for methicillin–resistant *Staphylococcus aureus* (MRSA). Released by Evanston Northwestern

Healthcare, the study finds that the majority of patients admitted harboring MRSA are not typically identified via passive or targeted active surveillance. Passive surveillance detects patients with clinical cultures only and is the method most commonly used for identifying MRSA in hospital patients in the U.S. Targeted active surveillance is used when particular areas of the hospital are labeled as high risk and all patients in those wards are screened. A second study conducted by the investigators characterized the decay pattern of MRSA colonization in a “real-life” population of retested patients in a universal surveillance and decolonization program. Results showed that re-colonization can occur, demonstrating the need for re-screening to detect re-colonization of patients upon each admission to the hospital. MRSA information: http://www.cdc.gov/ncidod/diseases/submenus/sub_mrsa.htm
Source: <http://www.infectioncontrolday.com/hotnews/6ah211471923058.html#>

27. *October 02, Public CIO* — **National Governors Association launches state Pandemic Preparedness Project.** As U.S. and international health officials continue to monitor the spread of the H5N1 avian flu, the National Governors Association Center for Best Practices (NGA Center) is launching a major effort to help states prepare for all aspects of a potential influenza pandemic. The Pandemic Preparedness Project will address the critical issues of public health preparedness, continuity of government planning, maintenance of essential services and the development of community-based and cross-border response strategies. The centerpiece of the project will be a year-long series of regional tabletop exercises, which will test federal, state and local preparedness; enhance coordination among all levels of government; build relationships among those responsible for critical decisions during a pandemic; and identify and rectify gaps in federal, state and local plans. Each exercise will involve state teams chosen by the governor and representing such functions as public health, homeland security, public safety, agriculture, education, emergency communications and the private sector. The NGA Center will publish after-action reports on each exercise and issue a final report on national pandemic preparedness at the close of the project.
Source: <http://www.public-cio.com/newsStory.php?id=2006.10.02-101360>

28. *September 28, Nature* — **Genomic analysis of increased host immune and cell death responses induced by 1918 influenza virus.** The influenza pandemic of 1918–19 was responsible for about 50 million deaths worldwide. Modern histopathological analysis of autopsy samples from human influenza cases from 1918 revealed significant damage to the lungs with acute, focal bronchitis and alveolitis associated with massive pulmonary edema, hemorrhage, and rapid destruction of the respiratory epithelium. The contribution of the host immune response leading to this severe pathology remains largely unknown. A recent study conducted by scientists from several institutions shows, in a comprehensive analysis of the global host response induced by the 1918 influenza virus, that mice infected with the reconstructed 1918 influenza virus displayed an increased and accelerated activation of host immune response genes associated with severe pulmonary pathology. It was discovered that mice infected with a virus containing all eight genes from the pandemic virus showed marked activation of pro-inflammatory and cell-death pathways by 24 hours after infection that remained unabated until death on day five. This was in contrast with smaller host immune responses as measured at the genomic level, accompanied by less severe disease pathology and delays in death in mice infected with influenza viruses containing only subsets of 1918 genes.
Source: <http://www.nature.com/nature/journal/vaop/ncurrent/full/nature05181.html>

Government Sector

29. *October 02, New York Times* — Amid fears of copycats, schools gird for security. Schools around the country were on alert Monday, October 2, after the second hostage taking, and third homicide case, in less than a week in a school. The killings in Nickel Mines, PA, with at least four students dead, occurred five days after a man took over a classroom in Colorado and killed one teenage hostage and himself as the police closed in. Some school administrators and security experts said that they were worried about a new pattern of violence for which schools were not well prepared — outside adults with grudges or suicidal urges entering schools — and that news coverage could inspire more crimes. School officials said the existence of a new pattern did not matter. Educators watch more closely the comings and goings in a school, they said, and they do the best they can. “It raises everybody’s awareness and reminds everyone to be vigilant, to never assume your school is going to be safe,” said Mike Vaughn, a spokesperson for the Chicago Public School System. Vaughn said that each of the 625 schools in his district had metal detectors, that 70 had full-time uniformed police officers and that the rest had off-duty police or security officers.

Source: <http://www.nytimes.com/2006/10/03/us/03copycat.html>

Emergency Services Sector

30. *October 03, Washington Post* — Drones expected to be new eye into little-seen part of hurricanes. Drones are better known for their role in pursuing military targets, but scientists in Boca Chica Key, FL, are poised to launch them into the raging vortexes of hurricanes. The small, unmanned aircraft will explore the storms at low levels that are too dangerous for “hurricane hunter” aircraft to probe. Meteorologists hope the information gathered will provide new details about wind speeds at the Earth’s surface and how a hurricane feeds itself on the warmth of the ocean. The drones, known as Aerosondes, have a wingspan of 10 feet and can be launched from an automobile with the aid of a rooftop launcher. The car, with a launcher strapped to the roof, reaches about 60 mph, at which point the aircraft is released by a latch. The planes are remarkably light, but also remarkably sturdy. Five Aerosondes are waiting in Florida for a hurricane to form. The \$300,000 for the project comes from NOAA and NASA.

Source: http://www.washingtonpost.com/wp-dyn/content/article/2006/10/02/AR2006100201063_pf.html

31. *October 02, NBC4 (Washington, DC)* — Surveillance cameras not living up to expectations. Many Washington, DC, police said they had hoped that installing dozens of new surveillance cameras across the city would assist them in cracking down on crime, but the system does not appear to be working as planned. It was a very violent weekend across the DC area, with 11 people shot, four of them fatally. One of the shootings in the District was caught on one of the new cameras, but police said so far, the cameras have not been much help in any other case. The incident remains under investigation. Community members said the shooting happened within yards of the cameras, which were of little deterrent. In some places trees limit what

cameras see. The surveillance program has been in effect for about a month, but police said there has yet to be prosecution involving evidence used from the cameras. The cameras, which focus on public space only, are "passively monitored" by the Metropolitan Police Department, meaning that officers generally do not watch the camera feeds in real time. The 48 surveillance cameras have been installed in communities that are considered high-crime areas throughout the city.

Source: <http://www.nbc4.com/news/9985252/detail.html?rss=dc&psp=news>

- 32. *October 02, Paisano (University of Texas at San Antonio)* — University receives \$95,000 grant for biometric pilot program.** The University of Texas at San Antonio (UTSA) received a grant to devise a biometric identification system to better identify firefighters when they report to an incident scene. The term "biometric" means something that is unique to oneself, such as voice patterns, fingerprints and facial dimensions. The researchers selected a fingerprint device for the biometric system, which would be most appropriate for firefighting conditions; facial and iris recognition are sensitive to lighting. Fire commanders would not only be able to keep better track of firefighters, but they could also recognize the firefighters' capabilities. The fingerprint authentication systems would be put on fire trucks and in firehouses, specifically on computer keyboards. Currently, firefighters are using a manual accountability system to identify themselves in which they take a piece of Velcro attached to their uniform and stick it onto a board at the scene. The \$95,000 grant is helping fund the pilot program in San Antonio at Fire Station 11.

Source: <http://www.paisano-online.com/vnews/display.v/ART/2006/10/02/452290eddfb40>

[[Return to top](#)]

Information Technology and Telecommunications Sector

- 33. *October 03, Security Focus* — Mozilla Firefox/Thunderbird/Seamonkey Multiple Remote Vulnerabilities.** The Mozilla Foundation has released six security advisories specifying vulnerabilities in Mozilla Firefox, SeaMonkey, and Thunderbird. These vulnerabilities allow attackers to: execute arbitrary code; perform cross-site scripting attacks; supply malicious data through updates; inject arbitrary content; execute arbitrary JavaScript; crash affected applications and potentially execute arbitrary code. Other attacks may also be possible. These issues are fixed in Mozilla Firefox version 1.5.0.7; Mozilla Thunderbird version 1.5.0.7; and Mozilla SeaMonkey version 1.0.5.

Solution: New versions of Firefox, SeaMonkey, and Thunderbird are available to address these issues. Referenced advisories for information on obtaining and applying fixes:

<http://www.securityfocus.com/bid/20042/references>

Source: <http://www.securityfocus.com/bid/20042/discuss>

- 34. *October 03, Register (UK)* — Unofficial patches defend against further IE flaw.** Two groups of security researchers have released unofficial patches designed to protect surfers against an outstanding Internet Explorer vulnerability in the absence of available security updates from Microsoft. The Zeroday Emergency Response Team (ZERT), a new ad-hoc group of security pros, released a patch designed to address a vulnerability in the browser's Active X controls last weekend. Security consultancy Determina published a separate fix for the same security bug in the WebViewFolderIcon ActiveX component of IE. The latest unofficial patches were released

in response to the availability of exploit code targeting the WebViewFolderIcon IE vulnerability, which creates a means to inject hostile code even on fully patched Win XP systems. Microsoft is working on a patch, currently scheduled for an October 10 release, as part of its regular Patch Tuesday update cycle.

ZERT patch: <http://isotf.org/zert/patch/ZProtector.zip>

Determina patch: http://www.determina.com/security_center/security_advisories/securityadvisory_0day_09282.asp

Source: http://www.theregister.co.uk/2006/10/03/zero-day_ie_fix_enco_re/

35. *October 03, SearchSecurity* — **Remote Firefox JavaScript flaw claim disputed.** One of the hackers who claimed to have found a new remotely exploitable JavaScript vulnerability in the popular Firefox browser has now said that claim was a joke and that no such flaw exists. Mischa Spiegelmock, one of two hackers who gave a presentation last weekend on Firefox flaws at a security conference called ToorCon, has told the Mozilla Foundation that the vulnerability he discussed cannot be used to execute arbitrary code. Instead, the flaw can only be used to cause the browser to crash and consume large amounts of system resources. At the conference, Spiegelmock and Andrew Wbeelsoi said they had discovered a previously unknown hole in Firefox's JavaScript implementation, which could allow a remote attacker to run code on a target machine. Window Snyder, who heads up Mozilla's security efforts, acknowledged at the time that there did seem to be a legitimate problem with the implementation. However, after looking at the code that the two hackers gave Mozilla, Snyder posted a message on the Mozilla Developer Center site Monday, October 2, saying that the problem is not as serious as Spiegelmock and Wbeelsoi claimed.

Source: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1219987,00.html

36. *October 02, Reuters* — **Screaming cell phones aim to cut down thefts.** A new phone security system may work to halt a spiraling rise in phone theft in the UK. The system sets off a high pitch scream, permanently locks the handset and wipes all data if reported stolen. The Remote XT technology, designed to make phones unusable and therefore worthless if they are stolen, works by installing software onto the operating system of the device that can be activated via a call to a call center once users realize their phone has been stolen or lost. The phone is then remotely disabled, all the data held on it is wiped and a high-pitched screech is triggered. According to UK government statistics, mobile phone theft has risen 190 percent in recent years, with one third of all UK robberies now solely involving mobile phones. The software currently works only on "smart phones" that run operating systems such as Symbian or Windows Mobile. But it is expected to be suitable for the majority of phones within two years.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003788&intsrc=news_ts_head

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	1026 (win-rpc), 4662 (eDonkey2000), 4672 (eMule), 65530 (WindowsMite), 32804 (---), 113 (auth), 445

(microsoft-ds), 25 (smtp), 139 (netbios-ssn), 135 (epmap)

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

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

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

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

Commercial Facilities/Real Estate, Monument & Icons Sector

37. *October 03, Detroit News* — Detroit police nab three suspects in copper theft. City police said on Tuesday, October 3, they have arrested three suspects in the theft of about \$400,000 in copper from two municipal facilities. The men were nabbed by undercover Detroit officers, part of a stepped up effort to crack down on the theft of valuable metals in the city. City officials estimate that in the past year more than \$7.5 million in damage has been done to city facilities by scrap scavengers. Two of the men were arrested about noon Sunday at the Brennan Pool in Rouge Park. They were found with saws and other tools. Police said they were removing copper wire, plumbing and fixtures and even showerheads and toilet seats at the pool.

Source: <http://www.detnews.com/apps/pbcs.dll/article?AID=/20061002/U PDATE/610020412>

38. *October 03, Anchorage Daily News (AK)* — Eielson experts defuse bomb found near trail. Explosives experts from Eielson Air Force Base in Alaska on Monday, October 2, deactivated what appeared to be a homemade pipe bomb found along a popular paved trail next to the Chena River. Now the deactivated device is in the hands of the FBI and Fairbanks police for further investigation, Fairbanks Fire Marshal Ernie Misewicz said. A crew that picks up trash on the trail found it in a plastic bag, put it in a pickup, and drove it to a parking garage, Misewicz said. Authorities immediately evacuated three major buildings associated with the garage — a courthouse, a high-rise senior housing complex and an apartment building, he said. The explosive experts then came and deactivated the device.

Source: <http://www.adn.com/news/alaska/story/8261311p-8158070c.html>

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

General Sector

Nothing to report.

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

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

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