



Department of Homeland Security

IAIP Directorate

Daily Open Source Infrastructure Report for 14 September 2004

Current Nationwide Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)

www.whitehouse.gov/homeland

Daily Overview

- The Los Angeles Daily News reports Southern California Edison officials on Sunday urged customers in Ventura and west Los Angeles county areas to conserve electricity after an equipment failure at a substation in Moorpark. (See item [3](#))
- The New York Times reports US Airways filed for bankruptcy protection on Sunday for a second time after workers refused to grant \$800 million in cuts it had sought to reduce its costs to the level of low-fare airlines; this means that two of the nation's biggest airlines are in bankruptcy court. (See item [10](#))
- News-Medical.Net reports the World Health Organization has warned that greater efforts will be needed if the world is to head off the threat of an avian influenza pandemic springing from the presence of the avian influenza H5N1 virus in poultry in Asia. (See item [20](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [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/IAIP Web 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://esisac.com>]

1. *September 13, Associated Press* — **Most power restored in affected counties.** Florida officials say 93 percent of the people who lost electric power due to Hurricane Frances now have their power back. **Emergency operations officials say there are still more than 217,000 customers without power in 27 counties as of Monday, September 13.** However, they say the power is 100 percent back in 35 counties that had reported some power outage after last

week's hurricane. Problems remain in some counties hardest hit by Frances, which include Brevard, Indian River and St. Lucie.

Source: <http://www.firstcoastnews.com/news/florida/news-article.aspx?storyid=24206>

2. *September 13, Bloomberg* — **Crude oil, natural gas rise as Ivan disrupts U.S. gulf output. Crude oil rose and natural gas soared in New York as the approach of Hurricane Ivan disrupted production and tanker shipments in the Gulf of Mexico, where a quarter of U.S. oil and natural gas is pumped.** Royal Dutch/Shell Group said completed evacuations on Monday, September 13, that idled 272,000 barrels of daily oil output. The Louisiana Offshore Oil Port, the biggest U.S. oil import terminal, said it stopped offloading tankers Monday. States along the Gulf receive more than half of U.S. oil imports and are home to 50 percent of the nation's refining capacity. Ivan's maximum sustained winds are close to 160 mph. Sunday, September 12, it was upgraded to a Category 5 storm, the National Hurricane Center in Miami, FL, said. **The expected path of the storm has been moving west the past three days, approaching oil-producing areas.** Ivan may hit the U.S. near the Alabama-Florida border early Thursday, September 16, forecasters said.

Source: <http://quote.bloomberg.com/apps/news?pid=10000006&sid=at8HSpJw02MU&refer=home>

3. *September 12, Los Angeles Daily News* — **Utility fears rolling blackouts. Southern California Edison (SCE) officials on Sunday, September 12, urged customers in Ventura and west Los Angeles, CA, county areas to conserve electricity after an equipment failure at a substation in Moorpark.** Tens of thousands of SCE customers in Moorpark, Simi Valley and Thousand Oaks lost power for at least an hour Saturday, September 11, after the substation failed, officials said. Other areas served by the substation included Calabasas, Malibu, Agoura Hills, Westlake Village and Newbury Park. Because of the failure of two of the substation's three transformers, SCE prepared to implement "an emergency rotating outage plan that will affect the surrounding communities for several days," according to a statement from SCE. **The malfunction involves two transformers used to convert higher voltages to levels used by homes and businesses. The cause remained under investigation, and it was unclear when the substation would be returned to full operation.** Gil Alexander of SCE said that if necessary, rolling blackouts — affecting about 5,000 customers at a time — will be called. The intention of the rotating outages is to avoid "a big impact on any one community at a time," Alexander said.

Source: <http://www.dailynews.com/Stories/0,1413,200~20954~2397676,00.html>

4. *August 13, Government Accountability Office* — **GAO-04-844: Electricity Markets: Consumers Could Benefit from Demand Programs, but Challenges Remain (Report).** The efficient and reliable functioning of the more than \$200 billion electric industry is vital to the lives of all Americans. As demonstrated in the 2003 blackout in the Northeast and the 2001 energy crisis in the West, changes in the cost and availability of electricity can have significant impacts on consumers and the national economy. The Federal Energy Regulatory Commission (FERC) supports using demand-response programs as part of its effort to develop and oversee competitive electricity markets. **Government Accountability Office (GAO) was asked to identify (1) the types of demand-response programs currently in use, (2) the benefits of these programs, (3) the barriers to their introduction and expansion, and (4) instances where barriers have been overcome. Additionally, GAO examined the federal**

government's participation in these programs through the General Services Administration (GSA). GAO recommends that (1) FERC consider demand–response in making decisions about wholesale markets and report to Congress on any impediments to doing so and (2) GSA make demand–response a key factor in its energy decision making. Highlight: <http://www.gao.gov/highlights/d04844high.pdf>
Source: <http://www.gao.gov/new.items/d04844.pdf>

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

Chemical Industry and Hazardous Materials Sector

Nothing to report.

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

Defense Industrial Base Sector

5. *September 14, Government Accountability Office* — **GAO–04–919: Defense Management: Tools for Measuring and Managing Defense Agency Performance Could Be Strengthened (Report).** The Government Accountability Office (GAO) was mandated to assess the effectiveness of defense agency performance contracts as management tools. As agreed, GAO also reviewed other tools (performance plans and balanced scorecards) and focused on three defense agencies—the Defense Logistics Agency (DLA), the Defense Information Systems Agency (DISA), and the Department of Defense Education Activity (DoDEA). GAO addressed (1) the extent that the defense agencies initially used performance contracts, including whether this tool addressed attributes associated with results–oriented management; (2) defense agencies' efforts to implement performance plans using lessons learned from the initial contracts; and (3) the extent the Department of Defense (DoD) established mechanisms to share lessons learned. GAO reviewed the content of these tools, but not the actual or reported performance. DISA has not yet finalized its scorecard, thus this report discusses only DISA's plans for its scorecard. GAO is making recommendations to DoD aimed at improving guidance to make performance plans and scorecards more informative and useful and further strengthen the potential of these tools for measuring and managing agency performance. In its comments, DoD generally concurred with GAO's recommendations. Highlights: <http://www.gao.gov/highlights/d04919high.pdf>
Source: <http://www.gao.gov/new.items/d04919.pdf>
6. *September 13, U.S. Northern Command* — **The CIFC helps thwart terrorist attacks. Combined Intelligence Fusion Center (CIFC) analysts pull together information from myriad sources to create an accurate, timely and clear picture of potential threats so North American Aerospace Defense Command (NORAD) and U.S. Northern Command (USNORTHCOM) can take action to deter, prevent and defeat threats against North America.** In addition to scanning, sorting and analyzing information, CIFC analysts also "fuse" the data with information from law enforcement agencies to try and "predict" threats. Because privacy rules prohibit the military from collecting information on U.S. citizens or information that does not have a "foreign threat nexus," analysts rely on intelligence collected by other legally authorized agencies, including the National Geo–Spatial Intelligence Agency, U.S.

Border Patrol and Department of Homeland Security. Just like USNORTHCOM, the CIFIC came into being following the September 11, 2001 terrorist attacks. Previously the center, known as the combined intelligence center, provided intelligence and warning analysis for foreign space, missile and air operations relevant to NORAD and U.S. Space Command. But after the terrorist attacks and the creation of USNORTHCOM, the CIFIC underwent a name and mission change.

Source: <http://www.northcom.mil/index.cfm?fuseaction=news.showstory&storyid=E4D81D56-EC5B-5516-D4A2118029AE1B4A>

7. *September 13, Associated Press* — **BAE agrees to buy DigitalNet for \$600M. British defense contractor BAE Systems PLC said Monday, September 13, it is buying DigitalNet Holdings Inc., a U.S. maker of secure computer networks and a leading information–technology supplier to the Pentagon.** BAE said its wholly owned U.S. subsidiary BAE Systems North America agreed to pay \$600 million in cash for DigitalNet and assume debt of \$93.25 million. BAE said the purchase will "enhance its ability to address evolving U.S. national security priorities for network centric infrastructure and information sharing between the intelligence, homeland security and warfighting communities." DigitalNet, which is headquartered in Herndon, VA, reported 2003 sales of \$336 million and employs some 2,200 people, mainly in the United States. BAE Systems, with 2003 sales of almost \$15 billion, employs some 90,000 people worldwide, including 26,000 in the United States.
Source: <http://www.nytimes.com/aponline/business/AP-Britain-BAE-DigitalNet.html>

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

Banking and Finance Sector

8. *September 13, eWeek* — **New scam tactic hits online. In the escalating clash between online scammers and security vendors, the attackers have once again developed new tactics that give them the upper hand in bypassing filters and infiltrating corporate networks, experts say. The new techniques, which experts began seeing sporadically earlier this year and in large waves in recent weeks, involve the use of a process called steganography, or embedding or hiding text in an image.** The most prominent example of the steganography wave is a recent variation on the ubiquitous Citibank phishing scam that attempts to lure recipients into disclosing online banking user names and passwords. Previous versions used text and images, such as authentic–looking Citibank logos and privacy seals. But versions that began surfacing recently are made up of one large image file containing all the text. While the subtle change is lost on most end users, the image–based messages are able to skirt most spam and content filters, which rely on algorithms that seek out certain text strings in spam or malicious e–mail. These filters, known as Bayesian filters, also consider the context of each e–mail but are unable to parse the text in the image files.
Source: http://www.eweek.com/print_article/0,1761,a=135038,00.asp
9. *September 12, The Arizona Republic* — **Computer files may be vulnerable to identity thieves. Personal computers seem to be an increasing target of choice for identity thieves seeking Social Security numbers, bank records and other sensitive personal information stored inside.** It is common for people to actively protect jewelry, artwork and other valuables, but it's equally wise to secure important papers, computer files and passwords, items used by

thieves to drain existing accounts and set up bogus new ones. Crooks also target businesses. In 2002, for example, they stole computers containing information on 562,000 military personnel and family members from TriWest Healthcare Alliance of Phoenix. This year, they took machines filled with personal data on nearly 34,000 credit-union members in California. Source: http://www.azcentral.com/arizonarepublic/business/articles/0_912Wiles12.html

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

Transportation Sector

10. *September 13, New York Times* — **US Airways tries to reorganize for a second time.** US Airways filed for bankruptcy protection on Sunday, September 12 for a second time after workers refused to grant \$800 million in cuts it had sought to reduce its costs to the level of low-fare airlines. **Nothing will change for US Airways customers right away, but few airlines have survived a second trip into bankruptcy court. The airline expressed confidence that it could reorganize under Chapter 11, but it is hobbled by limitations on its ability to find financing.** Over time US Airways may be forced to end service to some of the nearly three dozen cities where it is the only carrier. And if it fails to cut costs adequately, especially by winning concessions from workers, it may not survive, analysts said. **The filing means two of the nation's biggest airlines are in bankruptcy court.** United Airlines, the second-largest carrier after American, sought protection in December 2002 and has yet to emerge. Delta Air Lines, which is pressing its pilots to grant \$1 billion in wage and benefit cuts, has warned that it could also seek bankruptcy protection by the end of the month. Philip A. Baggaley, an airline industry analyst with Standard & Poor's, said there was little chance that US Airways would survive intact. The S. & P. put US Airways' credit rating into default. Source: <http://www.nytimes.com/2004/09/13/business/13air.html?pagewanted=all>
11. *September 10, Transportation Security Administration* — **TSA pledges \$6.5 million for explosives detection systems at Seattle-Tacoma International Airport.** Rear Adm. David M. Stone, USN (Ret.), Assistant Secretary of Homeland Security, Transportation Security Administration (TSA), today announced TSA has signed an agreement with the Port of Seattle for \$6.5 million. **The funds will help offset the cost of installing additional Explosives Detection Systems (EDS) machines, associated baggage handling system equipment, and Explosives Trace Detection (ETD) equipment. This explosive detection equipment will support an interim baggage screening solution at Seattle-Tacoma International Airport for Alaska Airlines.** "TSA continues to partner with the airports and airlines to deploy the most advanced technology that to ensure improved customer convenience and security," said Admiral Stone. TSA continues to work with Congress and the aviation community to deploy permanent baggage screening solutions for airports. TSA has authorized nearly \$1 billion for these efforts over the next three years. Source: http://www.tsa.gov/public/display?theme=44&content=090005198_00cba9e
12. *September 08, Business Travel News* — **BA selling Qantas stake. British Airways (BA), on September 8, informed Qantas of its intention to divest its 18.25 percent share in the Australian carrier, citing the need to lower debt and strengthen its balance sheet.** BA, which has held a piece of Qantas since 1993, expects the sale to generate more than A\$1 billion (US\$695 million). Both carriers said the transaction would have no impact on their existing

relationship, which includes sharing codes as part of mutual participation in the Oneworld alliance and an unrelated joint services agreement covering flight schedules, sales and operations between Australia, Southeast Asia, the United Kingdom and continental Europe. "A strong balance sheet will place British Airways in a robust position for any future European consolidation," said BA CEO Rod Eddington. BA currently is a minority shareholder in Spain's Iberia.

Source: http://www.btnmag.com/businesstravelnews/headlines/article_display.jsp?vnu_content_id=1000625711

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

Postal and Shipping Sector

13. *September 12, Associated Press* — Authorities narrow investigation into booby-trapped letters. Federal and state authorities have narrowed their investigation to a person of interest in the case involving at least 16 governors who were sent letters rigged to catch fire from a Nevada prison. "They have a focus for their investigation," Glen Whorton, assistant director for the Nevada Corrections Department, said Saturday, September 11. "They've narrowed it down to an individual." **Also Saturday, authorities confirmed that a 16th letter was sent to the office of Alaska Governor Frank Murkowski.** The letters apparently did not contain writings but bore a return address from Nevada's maximum-security Ely State Prison. In three cases, a match inside the envelope flared when the letter was opened, but no one was hurt. **The Montana Capitol was partly evacuated Thursday, September 9, when the match burned the letter opened there, but there was no further damage.** The letter sent to the office of Nevada Corrections Director Jackie Crawford contained blank paper and a match, which ignited as the paper was pulled out.

Source: http://www.napanews.com/templates/index.cfm?template=story_full&id=8DAD1EED-993C-4A5B-A329-0A80A137B790

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

Agriculture Sector

14. *September 13, Associated Press* — Japan confirms case of BSE. Japan has confirmed a new case of bovine spongiform encephalopathy (BSE), the third discovery of the brain-wasting illness in the country this year, an official said Monday, September 13. The five-year-old dairy cow tested positive for BSE, on Friday, September 10, at a slaughterhouse in Shisui town, in southern Kumamoto prefecture about 565 miles southwest of Tokyo, prefectural spokesperson official Toshinori Takano said. Officials at the agriculture and health ministries said they didn't know how many other dairy cows were at the sick animal's farm. Under a comprehensive screening system put in place after the outbreak three years ago, Japan tests every animal that is killed before it enters the food supply. Tokyo has also banned the use of meat-and-bone meal — made from ruminant animal parts — in cattle feed, which authorities believe led to the outbreak.

Source: http://www.aberdeennews.com/mld/aberdeennews/living/health/9_652153.htm

15. *September 13, Dow Jones Newswires* — **Brazil confirms foot and mouth disease.** Brazil's Ministry of Agriculture has confirmed an outbreak of foot and mouth disease (FMD) in the municipality of Careiro da Varzea, in the eastern region of Amazonas state located in the Amazon basin. **Tests conducted at a government laboratory confirmed that four head of cattle located on the property tested positive for the disease. The ministry has tested animals on neighboring farms and is trying to restrict movement of livestock in the region.** The region produces beef for local consumption only, and given the isolated location of the municipality, it's unlikely the disease will spread to other regions, the ministry said. Brazil has the world's largest commercial cattle herd.

Source: http://www.agprofessional.com/show_story.php?id=27334

16. *September 13, Orlando Sentinel (FL)* — **Florida agriculture losses. From the inundated cattle pastures of Polk County to the shredded ferneries in Volusia, hurricanes Charley and Frances may have handed Florida's agricultural industry its most costly double shot ever: preliminary estimates put losses at more than two billion dollars** Growers, ranchers, and farmers have been working around the clock to care for animals, repair fences, and reconstruct buildings. **The already staggering numbers are still growing. Losses were \$200 million for citrus, \$50 million for vegetable growers, and more than \$400 million for nurseries. And even before Frances arrived, 63 percent of Florida ranches had been significantly damaged.** This is the time of year when ranchers sell their cows at market — yet five of 10 auction houses in Florida were closed last week because of Hurricane Frances. Meanwhile, cows graze in swamped pastures with less nutritious grass to eat and more mosquitoes to chase them, driving down their weight. About 80 percent of the state's 1.2 million head of cattle has been affected to some extent by the two storms. Osceola and Polk counties are two of Florida's biggest cattle producers and the two Central Florida counties hardest hit by Charley.

Source: http://www.sun-sentinel.com/business/local/sfl-913canecitrus_0.352109.story?coll=sfla-business-headlines

17. *September 12, Associated Press* — **Sensors gather harvest data.** Tiny sensors planted in a sugar beet field south of Fargo, ND, gather data vital to helping the crop reach its harvest potential. Smart dust is the industry tag given to radio frequency identification technology taken to a new level. The same technology that will reshape the retail world — replacing UPC codes with tiny transmitters — is expected to invade all aspects of commerce through the use of wireless sensor networks. Smart dust sensors not only provide information about location, but gather data and deliver it via antennas to the Internet. **The sensors are set just beneath the knee-high leaf canopy protecting the beet. Every five minutes the sensors read and relay to a computer, readings on temperature, humidity, leaf wetness, and soil moisture.** Al Cattanach, a field agronomist with American Crystal, said accurate and timely data from a field could result in big savings for growers. An application of fungicide or fertilizer costs about \$20 an acre. Spread among American Crystal's 500,000 acres, eliminating just one treatment based on field information could result in \$10 million in savings, he said. Timely data can help growers prevent disease to plants, Cattanach said. The North Dakota Agricultural Statistics Service has less-specific data stations set up on a county-by-county basis. While the information can be a guide to growers, it can't tell them exactly what's taking place in their field.

Source: http://wcco.com/localnews/local_story_256105535.html

18. *September 11, Associated Press* — **WSU veterinary hospital fights terror. The Washington State University (WSU) College of Veterinary Medicine is on the front lines of the war on terrorism, part of a nationwide early warning system to detect if bioterrorists have struck the U.S.** Last February, President Bush ordered the federal government to develop new procedures to protect the nation's food supply from terror attack. He called for creation of systems to contain any outbreaks of plant or animal disease that result from terror attack, and to prevent or cure the diseases themselves. It is vets who must fight those threats. If terrorists try to contaminate cattle, poultry or other farm animals, Terry McElwain, director of the Washington Animal Disease Diagnostic Lab, would be among the first to know. The lab, created in 1974, can quickly perform tests on thousands of samples. **After the terrorist attack on September 11, the WSU lab became one of 12 in a national network responsible for spotting exotic disease outbreaks in animals. That includes potential "agroterrorist" weapons like foot and mouth disease, swine fever, avian flu, and others, plus lethal disease such as Ebola, plague, and tularemia.** The vet hospital also has its own SWAT team, a field disease unit. The unit can move on short notice to the scene of unexplained animal deaths such as cows dropping in fields, or large numbers of chickens expiring in their coops.
Source: <http://www.casperstartribune.net/articles/2004/09/12/news/regional/fd25db000fd3b59f87256f0d00055385.txt>

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

Food Sector

19. *September 13, Dow Jones Newswires* — **Ukraine lifts Texas poultry ban. Ukraine has lifted a ban on poultry products imported from Texas, six months after restricting imports over fears of the highly contagious bird flu, Ukrainian officials said Monday, September 13.** The veterinary department at Ukraine's Agriculture Ministry said the ban on live birds, meat, and eggs and all poultry byproducts was lifted September 7. **The ban on poultry from two other states, Maryland and Delaware, remains in effect, officials said.** Ukraine last December ended an 11-month ban on U.S. chicken and began accepting shipments certified to contain no growth stimulants, hormones, or other banned additives. Before the ban, U.S. producers supplied about 90 percent of Ukraine's chicken imports.
Source: http://www.agprofessional.com/show_story.php?id=27336

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

Water Sector

Nothing to report.

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

Public Health Sector

20. *September 13, News-Medical.Net* — **Growing global threat from avian influenza. The World Health Organization (WHO) has warned that greater efforts will be needed if the**

world is to head off the threat of an avian influenza pandemic springing from the presence of the avian influenza H5N1 virus in poultry in Asia. "Unless intensive efforts are made, a pandemic is very likely to occur," Dr Shigeru Omi, WHO's Regional Director for the Western Pacific, told a news conference in Shanghai. The H5N1 virus causing avian influenza among poultry in Asia is circulating more widely than initially believed, Omi said. **The cyclical history of previous influenza outbreaks means a pandemic is due, and virtually nobody would be immune to a new human influenza virus that resulted from outbreaks in poultry, he said.** Also of concern is the increased global movement of people and goods means the virus could spread far more quickly and extensively than in the past. Since the first reported outbreaks of avian influenza in Asia at the beginning of this year, there have been 39 confirmed human cases in the region, 28 of whom died. The latest case was on September 8, when an 18-year-old man died in eastern Thailand. H5N1 has been confirmed in nine Asian countries, where tens of millions chickens have died or been slaughtered.

Source: <http://www.news-medical.net/?id=4729>

21. *September 13, Scientific American* — **Nipah virus may spread between people. In February the Nipah virus reemerged, killing 35 people in Bangladesh in two outbreaks. The deaths have health officials worried. Unlike its first appearance in Malaysia in September 1998, the virus in Bangladesh may have jumped from person to person, raising concern about its ability to spread farther and faster.** Nipah is a henipavirus. Distant relatives of measles, henipaviruses appear to reside naturally in flying foxes, the world's largest bats. The virus spreads through bodily fluids such as saliva or urine. Flying foxes live across the Pacific lands and Africa. Roughly a third of those in Malaysia and Australia harbor antibodies against the infections, suggesting that the bats and viruses evolved together. In contrast to its original outbreak in Malaysia, which claimed nearly 40 percent of those infected, the mortality rate of the Bangladeshi outbreaks was 74 percent. It is unclear is how the Bangladeshi patients became infected. Previously Hendra and Nipah leaped from bats to humans via intermediate animal hosts. Victims in the first Nipah outbreaks, for instance, caught the sickness from pigs. Many victims in Bangladesh, however, had no direct contact with animals, and no infected domestic animals were seen. **Human-to-human transmission would also make henipaviruses even more desirable to bioterrorists.**

Source: <http://www.sciam.com/article.cfm?chanID=sa004&articleID=0006321E-8ECD-111B-87CB83414B7F0000>

22. *September 12, Detroit News (MI)* — **Network links health care workers.** Until recently, doctors, nurses, and other health care workers across Michigan couldn't warn each other of a bioterrorism attack or infectious disease outbreak. Today, 2,000 health officials throughout the state can sound an alarm instantly through a network that always knows exactly how to find the right people — office phone, cell phone, home phone, pager or e-mail — and confirms that they get the alert. **The Michigan Health Alert Network links every hospital and local health department statewide through a software program called Virtual Alert.** "If you have an action that needs to be taken on an outbreak of meningitis in kids, you don't want people to not get notification over the weekend, when perhaps they need to start vaccinating or looking at cases," said Jackie Scott, director of the state's Office of Public Health Awareness. **In March, when a man who traveled through Detroit Metropolitan Airport on his way from India to Iowa was found to be infected with measles, a community health official activated the network from his home computer at 9 p.m. on a Saturday. Within two hours, officials**

from 26 of the state's 45 health departments had confirmed that they received the alert. Everyone with access to the network has the ability to activate it. Messages sent through the network can be targeted to specific geographic areas and priority designated.

Source: <http://www.detnews.com/2004/business/0409/12/d04-270837.htm>

23. *September 12, Washington Post* — Fears about smallpox shots may put public at risk. Since President Bush helped launch a smallpox preparedness program in 2002, local health officials say they have come a long way in developing plans to vaccinate the Washington, DC, region's entire population in the event of an outbreak. Officials remain concerned about security, shortages of trained staff, and the challenge of calming a populace likely to be terrified. **Perhaps the greatest hurdle continues to be a lack of health care workers and first responders willing to become vaccinated. Nationwide, only about 40,000 of them have received the vaccine, way short of the initial target of 500,000, according to the Centers for Disease Control and Prevention.** Officials said people are reluctant to volunteer to be vaccinated because of risks associated with the vaccine. And the risk of an actual outbreak has been seen as increasingly remote, health officials said, further limiting volunteers. **The lack of response from the medical community most likely means that vaccination of the general public would be delayed in the event of an outbreak. Those health officials and emergency workers who previously declined probably would be vaccinated first,** costing precious time, said Julie Casani, director of public health preparedness for the Maryland Department of Health.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A14556-2004Sep11.html>

24. *September 12, Associated Press* — Thai children show bird flu symptoms. Four Thai children were hospitalized Sunday, September 12, with symptoms of avian flu, a health official said, days after the disease claimed its latest human victim since resurfacing in Asia two months ago. Two boys, aged six and eight years, and a three-year-old girl were hospitalized with fevers and coughs in the Krabin Buri district of Prachinburi province, said Charal Trinvuthipong, director-general of the Health Ministry's Department of Communicable Disease Control. A two-year-old girl in Bangkok's Minburi district was also hospitalized to be monitored for the virus, he said. The lethal H5N1 strain of avian influenza devastated poultry farms across Asia at the start of the year, killing or forcing authorities to slaughter tens of millions of birds before it re-emerged in July. The disease has infected humans and killed a total of 28 people in Vietnam and Thailand this year.

Source: http://seattlepi.nwsource.com/national/apasia_story.asp?category=1104&slug=Thailand%20Bird%20Flu

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

Government Sector

Nothing to report.

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

Emergency Services Sector

25. *September 13, Federal Computer Week* — **Responders want nationwide interoperable communications.** During a Wednesday, September 8, congressional hearing, a panel of state and local officials had a list of problems — such as lack of money, planning, coordination, guidance, training, and expertise; outdated equipment and technology; limited radio spectrum; and uneven procurement cycles — that surround the homeland security issue in many communities. **But many also said the Safecom office — a federal program within the Homeland Security Department that is establishing national standards and architecture and coordinating federal activity regarding communications interoperability — is actually working well with communities to resolve such issues. They said Safecom officials understand that interoperability should be locally driven and not from the top down.** They requested continued support for the office. Michael Neuhard, chief of the Fairfax County, VA, Fire and Rescue Department, said communities surrounding the metropolitan Washington, DC, area have addressed the issue of interoperability for many years and also have received continued funding since the September 11, 2001, attacks. But he said first responders are concerned about communities farther away from metropolitan areas that would need to be called on should another catastrophic event occur.
Source: <http://www.fcw.com/geb/articles/2004/0906/web-interop-09-10-04.asp>
26. *September 13, Associated Press* — **New communications tool for emergency responders. New "Safety Web" technology unveiled in Rochester, NY, on Monday, September 13 is aimed at enabling first responders to share critical information and talk with each other in case of emergencies.** The new tools allow emergency responders and government officials to almost instantly set up online communications over the Internet. Police and firefighters can all share critical information instantly, whether it's text, voice or video. Western New York Congresswoman Louise Slaughter says the new technology could lead to a nationwide fix for one of the biggest problems faced during the September 11, 2001 terrorist attacks — the inability of police and firefighters to talk with each other and with government officials.
Source: <http://www.wstm.com/Global/story.asp?S=2294005>
27. *September 13, Los Alamos Monitor* — **9/11 changed state's outlook.** Three years after the September 11 terrorist attacks, New Mexico's Homeland Security head Dr. Annette Sobel assesses the state's emergency preparedness and is pleased with what she sees. "The Governor's Office of Homeland Security has made significant progress in the areas of information sharing and risk management to ensure our state's critical infrastructure is protected," Sobel said. **The infrastructure includes government buildings, the state capitol, highways, telephone lines and things of that nature, she said.** "New Mexico has also taken a lead role in facilitating border security partnerships and enhanced emergency responsiveness between the United States and Mexico along our adjoining border," Sobel said. "We have worked through the governor's border initiative and are working with the U.S. Border Patrol and U.S. Customs to ensure the safety of our borders." Timothy Manning, New Mexico's Office of Emergency Management director said **the federal funding is used to increase the training level of local and state responders, fill the shortfall in bomb team, Hazmat, and weapons of mass destruction responder equipment and to purchase special security tools to detect chemical agents in the atmosphere.**
Source: http://www.lamonitor.com/articles/2004/09/13/headline_news/news02.txt

28.

September 10, Firehouse.com — **Grants to firefighters aid hundreds of departments.** On Friday, September 10, Department of Homeland Security Secretary Tom Ridge announced 343 grants to fire departments throughout the United States in the fifteenth round of the Fiscal Year 2004 Assistance to Firefighters Grant Program. The grants will ultimately total approximately 8,000 awards worth nearly \$750 million in direct assistance to firefighters throughout the country, demonstrating Homeland Security's commitment to ensuring that America's firefighters have the resources they need to protect their communities. **This fifteenth round of grants provides \$23,096,556 to help local fire departments purchase firefighting equipment, fund firefighter health and safety programs, enhance emergency medical services programs, and conduct fire education and prevention programs.** The Assistance to Firefighters Grant Program is administered by the Department of Homeland Security's Office for Domestic Preparedness in cooperation with the Department's United States Fire Administration.

Source: http://cms.firehouse.com/content/article/article.jsp?section_Id=46&id=34967

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

Information Technology and Telecommunications Sector

29. *September 13, InformationWeek* — **Technology can help fight the growing cyberextortion threat, but experts say not enough companies are prepared.** A survey by Carnegie Mellon University, in conjunction with InformationWeek, found extortion attacks are surprisingly common: **17% of the 100 companies surveyed say they've been the target of some form of cyberextortion, such as a threat to disable their website or reveal confidential information.** The findings come as no surprise to FBI special agent Thomas Grasso, who helped with the study. "The majority of the cybercrimes we investigate involve some type of monetary motivation," Grasso says. While most extortion plans fail (70% of those threatened with extortion say the attempts were unsuccessful), cyberextortion is a growing problem. Networks with large numbers of compromised systems that can be used to launch distributed denial-of-service attacks have increased sharply this year, says Vincent Weafer, senior director of Symantec Corp.'s Security Response service. **Many companies aren't taking necessary precautions. Only 21% of companies in the Carnegie Mellon study have formal training programs to teach employees how to respond to security breaches, and only 37% have performed security assessments in the past six months.** More information on the study is available at: <http://www.andrew.cmu.edu/user/gbednars/>
Source: <http://www.informationweek.com/story/showArticle.jhtml?articleID=47204212>

30. *September 13, Seattle Post-Intelligencer* — **Dozens of experts take on cyberterror.** Government and business experts in security and critical infrastructure gathered last week in Seattle, WA, to uncover vulnerabilities to a cyberterror attack that could cause basic services, such as electricity, water and banking to crash. **While computer technology increases efficiency and productivity across the spectrum of human endeavors, it also provides an access point for cyberterrorists to disrupt telecommunications, utilities and other major systems in profound ways.** For example, dams, electric distribution grids, municipal water supplies and gas pipelines are all remotely controlled by computerized systems that relay orders to open and close distant switches and valves. **A cyberterrorist able to hack into such a system could cause chaos by opening a dam spillway or shutting down a high-voltage**

power line. Last week's exercise was designed to explore the interdependencies among these various sectors. Acknowledgment of those interdependencies and the vulnerabilities they create brought to the table more than 100 experts from Seattle, several states, the Department of Homeland Security, the Navy, Army and Marine Corps, Microsoft, Boeing, the FBI, numerous U.S. and Canadian utilities, the Bonneville Power Administration and the Los Alamos, Sandia and Argonne national laboratories. The cyberterror simulation, dubbed Blue Cascades II, was convened by the Pacific NorthWest Economic Region.

Source: http://seattlepi.nwsourc.com/local/190473_cyberterror13.htm

31. *September 13, The Register (UK)* — **Multipurpose Internet Mail Extensions (MIME) protocol vulnerabilities.** The UK's National Infrastructure Security Co-ordination Centre (NISCC) warned on Monday, September 13, of a series of vulnerabilities involving implementations of the Multipurpose Internet Mail Extensions (MIME) protocol within e-mail and web security products. NISCC's advisories warn how malformed MIME constructs might be exploited to allow attackers to bypass content checking and anti-virus tools. MIME is a standard method for encoding e-mail attachments so the extent of the problem highlights a security hole that might be used by virus writers to smuggle hostile code past security defenses. Original advisory: <http://www.uniras.gov.uk/vuls/2004/380375/mime.htm>
Source: http://www.theregister.co.uk/2004/09/13/mime_vuln/
32. *September 12, SecurityTracker* — **Serv-U FTP Server vulnerability.** A vulnerability exists in Serv-U FTP 4.x and 5.x which can allow remote authenticated users to crash the target FTP server with STOU commands. There is no vendor solution currently available.
Source: <http://www.securitytracker.com/alerts/2004/Sep/1011219.html>
33. *September 10, Federal Computer Week* — **HSARPA seeks cyberdefense R&D.** Officials at the Homeland Security Advanced Research Projects Agency (HSARPA) released a broad agency announcement last week about the development and deployment of technologies to protect the nation's critical cyberinfrastructure. **Officials in the agency's Cyber Security Research and Development program hope to improve the security of current and emergency technologies and systems; develop new and enhanced technologies to detect, prevent and respond to cyberattacks; and transfer such technologies into the national infrastructure.** Officials at HSARPA, which is part of the Homeland Security Department's Science and Technology Directorate, expect as much as \$4.5 million will be available for multiple awards under this solicitation. Officials will announce the awards January 18, 2005.
Source: <http://www.fcw.com/fcw/articles/2004/0906/web-hsarpa-09-10-04.asp>
34. *September 10, SecurityTracker* — **Apache mod_ssl denial of service vulnerability.** A vulnerability was reported in Apache mod_ssl 2.0.50 when used as a reverse proxy. A remote user can cause denial of service conditions in a certain configuration. A fix is available via CVS at http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.125&r2=1.126
Source: <http://www.securitytracker.com/alerts/2004/Sep/1011213.html>
35. *September 10, US-CERT* — **US-CERT Vulnerability Note VU#490708: Microsoft Internet Explorer window.createPopup() method creates chromeless windows.** The Internet Explorer (IE) window.createPopup() method creates chromeless pop-up windows which can be

used to spoof the user interface in Internet Explorer, any Windows application, or the Windows desktop. By convincing the user to view an HTML document (web page, email message) an attacker can deceive the user by changing the appearance of the GUI. Refer to US-CERT Vulnerability Note for workarounds.

Source: <http://www.kb.cert.org/vuls/id/490708>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis	
Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.	
US-CERT Operations Center Synopsis: The US-CERT Operations Center strongly encourages Windows XP users to upgrade to Service Pack 2 if they have not already done so. SP2 offers significant protection against many of the emergent attacks that target Browser Helper Objects and Cross Domain Vulnerabilities in Internet Explorer. See http://www.us-cert.gov/cas/alerts/SA04-243A.html for more information.	
Current Port Attacks	
Top 10 Target Ports	135 (epmap), 445 (microsoft-ds), 1434 (ms-sql-m), 139 (netbios-ssn), 137 (netbios-ns), 6129 (dameware), 9898 (dabber), 5554 (sasser-ftp), 1433 (ms-sql-s), 1026 (nterm)
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

36. *September 13, WXIA-TV (GA)* — Suspicious device found at school. A bomb squad blew up a suspicious device found at a Gwinnett County high school in Lawrenceville, GA, on Monday, September 13, authorities said. The device was discovered in a small courtyard at the high school. School spokesperson Sloan Roach said only students in the immediate area were evacuated until the scene was declared safe. The exact nature of the device has not been confirmed.

Source: http://www.11alive.com/news/news_article.aspx?storyid=51826

[[Return to top](#)]

General Sector

Nothing to report.

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Alerts](#) – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues.

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644 for more information.

Contact DHS/IAIP

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.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.