



Department of Homeland Security Daily Open Source Infrastructure Report for 22 February 2007

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- SC Magazine reports phishers are using Google Maps and IP addresses in a new social engineering attack for committing identity theft, targeting customers with Bank of America accounts in the United States and account holders with other financial institutions in Australia and Germany. (See item [8](#))
- The Department of Homeland Security has announced the launch of the Traveler Redress Inquiry Program, which allows travelers to seek redress and resolve possible watch list misidentification issues with any of the department's component agencies at an easy to use and easy to access online location. (See item [14](#))

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. *February 21, Bloomberg* — **Oil rises above \$60 on concern refinery curbs may trim supply.** Crude oil rose above \$60 a barrel in New York on concern that unexpected refinery shutdowns will curb fuel stockpiles in the weeks ahead. Fires and interrupted power supplies trimmed output at refineries in Texas, Pennsylvania, Colorado, Ontario and Delaware over the past two weeks. A pipeline supplying the U.S. Midwest and Northeast cut shipments. An Energy Department report may show that U.S. supplies of distillate fuel, which includes diesel and

heating oil, fell last week, a Bloomberg News survey showed. A Teppco Partners LP pipeline in a rural area near Batesville, IN, was shut Tuesday, February 20, after a diesel spill, a spokesperson said. The pipeline carries refined petroleum products including diesel, gasoline and jet fuel from the Gulf Coast into the Midwest and Northeast. Colonial Pipeline Co. will ration space for distillate–fuel shipments on a line running from Collins, Mississippi, to Greensboro, North Carolina. Valero Energy Corp.'s McKee refinery in Texas was shut on February 16 because of a fire. Mary Rose Brown, spokesperson for the San Antonio–based company, said Tuesday it will be several weeks before a partial resumption of operations at the plant. The refinery has a processing capacity of 170,000 barrels a day.

Source: <http://www.bloomberg.com/apps/news?pid=20601087&sid=aHxN5sj9Km50&refer=home>

2. *February 20, Associated Press* — **BP's Northstar oil field shut down after gas leak discovered.** BP PLC shut down an offshore oil field in the Arctic Ocean after a small leak in a gas line was detected, a company official said Tuesday, February 20. The shutdown of the Northstar oil field has taken about 40,000 barrels of oil offline each day since Friday or Saturday, said BP spokesperson Daren Beaudou. Beaudou said he was not sure when the field would resume operations. There was no environmental damage and no safety hazard associated with the leak, found in an eight–inch pipe used to handle extraneous gas from the field, Beaudou said. The pinhole–sized leak was discovered during a routine inspection of Northstar's wells and processing facilities, which sit atop a man–made gravel island six miles off the northern coast of Alaska. The 27–square–mile field is located 39 feet beneath the ocean surface.

Source: http://seattletimes.nwsources.com/html/nationworld/2003580950_webbp20.html

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

Chemical Industry and Hazardous Materials Sector

3. *February 21, Longview News–Journal (TX)* — **Truck wreck causes diesel leak.** The driver of an 18–wheeler said he was unsure how he lost control of his truck Tuesday morning, February 20, causing it to jackknife off Texas 149 and spill about 100 gallons of fuel in southeast Gregg County. An investigating Department of Public Safety trooper said wet roads and failure to control speed were the likely causes of the one–vehicle wreck in the northbound lane across from Cherokee Water Co. As the truck left the road, it ran over a highway reflector pole, puncturing the gas tank. A hazardous materials team was called to clean up leaking diesel. Although traffic did not come to a halt, it was slowed as Lakeport police directed vehicles around the wreck.

Source: http://www.news–journal.com/news/content/news/stories/022120_07_149_wreck.html

4. *February 20, Ledger (FL)* — **Fire in Pepsi plant prompts highway closure.** A fire with possible environmental damage that closed down a portion of Recker Highway broke out at a Pepsi–Cola bottling facility Monday afternoon, February 19. The fire, at 5023 Recker Highway in Winter Haven, FL, started about 3:30 p.m. EST in the maintenance section of the small bottling plant. "There was one drum of waste oil in the maintenance area that ruptured," said Mike Linkins, spokesperson for Polk County Fire/Rescue, as well as a pallet of batteries that leaked acid, fueling the blaze. The blaze took about 45 minutes to put out. The Polk County Sheriff's Office shut down Recker Highway for about an hour and a half in both directions

because a large fire hose had to be laid across the road to connect to a fire hydrant. The road was reopened about 5 p.m. EST.

Source: <http://www.theledger.com/apps/pbcs.dll/article?AID=/20070220/NEWS/702200353/1134>

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

Defense Industrial Base Sector

5. *February 21, National Defense* — **Army seeks light, efficient batteries to meet insatiable energy demand.** In an Army that heavily depends on battery-operated devices to do its job, the complaints are well documented: Batteries are too heavy, too bulky and not very user-friendly. All that could change, if Steve Slane has his way. Slane, chief of the battery branch at Army Communications-Electronics Research, Development and Engineering Center (CERDEC) at Fort Monmouth, NJ, is working with several contractors to develop new battlefield batteries — an effort employing 30 Army scientists and engineers and budgeted at around \$15 million annually. In today's high-tech Army, where even the smallest patrol counts on a wide range of electronic systems, batteries are a critical resource. And demand is growing. "Five to 10 years ago, a soldier on average would consume three to four watts of [battery] power" on a typical mission, Slane says. "Today...we're seeing power numbers of around 20 watts." To provide 20 watts, a soldier might carry as many as eight 2.2-pound BA-5590 lithium sodium dioxide batteries on a mission, in addition to smaller alkaline batteries, for a combined weight of around 20 pounds. As a result, battery weight and size have become important factors in mission planning.

Source: http://www.nationaldefensemagazine.org/issues/2007/February/A_rmyseeks.htm

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

Banking and Finance Sector

6. *February 21, Websense* — **Trojan horse bots allow attackers to compromise end-user banking credentials.** Websense Security Lab has received reports of new malicious Websites designed to install Trojan Horse bots that allow attackers to compromise end-user banking credentials for more than 50 financial institutions and ecommerce Websites. The Websites are hosted in Germany, England, and Estonia, and appear to be using round robin DNS, resolving to five unique IP address that revolve on each lookup. Each site hosts the same exploit code. When end-users visit the site, they are directed to one of the five servers. If the end-user machine is vulnerable, a file called "iexplorer.exe" is downloaded and run. The site displays a simple page that says the sever is temporarily busy and suggests that the user shut down any firewall and antivirus software. The "iexplorer.exe" file downloads and installs five additional files from a server in Russia.

Source: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=743>

7. *February 21, Websense* — **Phishing Alert: Party Poker.** Websense Security Labs has received reports of a phishing attack that targets users of Party Poker. Users receive a spoofed email message which claims that a new online gambling law will be passed, and that they must

log in to their account to view the impact on Party Poker users. The email provides a link to a phishing site that attempts to collect personal and account information. This phishing site is hosted in the United States.

Source: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=744>

8. *February 21, SC Magazine* — **Phishing attack use Google Maps, IP addresses to obtain victim location.** Phishers are using Google Maps in a new social engineering attack for committing identity theft. Customers with Bank of America accounts in the United States and account holders with other financial institutions in Australia and Germany have been targeted by the attacks, according to published reports. Attackers have spread keylogger malware through a fake news report of Australian Prime Minister John Howard suffering a heart attack. After duped users clicked on an included link, PCs were infected with keylogger trojans capable of allowing a hacker to track a victim's IP address and find the his or her general location. That information can then be used for identity theft, according to researchers. Ron O'Brien, senior security analyst at Sophos, said that fraudsters can use the information gathered through the IP address and Google Maps to create a profile of the person they're looking to scam.

Additional information is available from Websense:

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=741>

Source: <http://scmagazine.com/us/news/article/634718/phishing-attack-use-google-maps-ip-addresses-obtain-victim-location/>

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

Transportation and Border Security Sector

9. *February 21, Associated Press* — **Planes evacuated after getting stuck at National Airport.** Officials at Reagan Washington National Airport in Arlington, VA, are trying to determine why two commercial airliners wound up on closed taxiways on Tuesday night, February 20. The incidents involved a Northwest Airlines plane from Memphis that turned onto a taxiway and got stuck in ice that had not been cleared since last week's winter storm, and a United Airlines flight that turned onto a different taxiway and got stuck. Airport spokesperson Robert Yingling says in both cases, shuttle buses and fire department vehicles cruised over the tarmac to the stranded airliners and passengers were safely evacuated.

Source: http://www.wusa9.com/news/news_article.aspx?storyid=56076

10. *February 21, USA TODAY* — **Two more flights abandoned fliers on way to Denver.** In a second recent incident of its kind, about 100 passengers on two airline flights diverted from Denver because of bad weather were left behind at a Nebraska airport on February 8. Darwin Skelton, airport manager at Scottsbluff, NE, said crews of United Express and American Connection flights left the passengers behind about six hours after landing. The flights, from Madison, WI, and St. Louis were diverted to Scottsbluff because of fog in Denver. The incident occurred less than two months after two United Express jets diverted to Cheyenne, WY, after a blizzard hit the Denver airport December 20 and left without their passengers. In Scottsbluff, some passengers rented the few Hertz cars available at the airport, but most later that night boarded a Denver-bound charter bus arranged by Hertz. Both planes in the Nebraska incident were operated by St. Louis-based Trans States Airlines, which operates flights under contract

with American, United and US Airway

Source: http://www.usatoday.com/money/biztravel/2007-02-20-airport-a-bandoned-usat_x.htm

11. *February 21, Associated Press* — **US Airways passengers' baggage delayed.** Some US Airways passengers who flew through Philadelphia during last week's nasty winter storm still didn't have their luggage by Tuesday, February 20, an apparent step back for a company battling persistent baggage complaints. US Airways canceled 670 flights into and out of Philadelphia as a major winter storm hit the Northeast last week. Thousands of bags were separated from their owners. On Tuesday morning, at least 200 bags were still lined up in the baggage claim area at Philadelphia International Airport. US Airways has been trying to improve its baggage handling after a meltdown about two years ago. Over three days in December 2004, the airline had to cancel hundreds of flights and thousands of pieces of luggage were stranded in Philadelphia after scores of flight attendants and baggage handlers called in sick. The company just pumped \$20 million in upgrades for its Philadelphia airport facilities, including new baggage-handling equipment.
Source: http://biz.yahoo.com/ap/070220/us_airways_baggage.html?.v=1
12. *February 21, Brazil Magazine (CA)* — **U.S. Air Line Pilots Association warns about Brazil's dangerous airspace.** The U.S.-based Air Line Pilots Association, International, (ALPA) has just released an alert to its members on the difficulties of operating in the Brazilian airspace stressing the limited knowledge of the English language by Brazil's flight controllers. The association warns that pilots should maintain a high level of awareness while operating in Brazil. According to ALPA's document, which was written on January 29, the collision of the executive Legacy jet with the Gol's Boeing 737, over the Amazon, on September 29, which killed all 154 people aboard, "has highlighted several issues associated with operations in that airspace that may have significant implications for the safety of flight." The Brazilian Air Force says it has already taken steps to solve the problems dealing with flight security in the country and one of the measures was to enroll controllers in English's courses.
ALPA report: see source
Source: <http://www.brazilmag.com/content/view/7922/54/>
13. *February 21, WABC (NJ)* — **NJ Transit train derails during commute.** New Jersey Transit suspended three employees and ordered additional railroad switch inspections after a train derailed during the commuter morning rush on Wednesday, February 21. The train was heading from Waldwick to Hoboken at the height of rush hour when it derailed in Ridgewood. Three coaches of a five car New Jersey Transit train derailed. Officials say approximately 100 passengers were on board. A track supervisor and two track foremen were suspended without pay pending an administrative hearing. Within 24 hours, NJ Transit also said it will inspect four similar switches installed in the last year. The train was traveling 36 mph when it crossed over from the Main Line to the Bergen County Line, which is lower than the 45 mph authorized speed limit a spokesperson said.
Source: <http://abclocal.go.com/wabc/story?section=traffic&id=5055013>
14. *February 21, Department of Homeland Security* — **DHS launches Traveler Redress Inquiry Program.** The Department of Homeland Security (DHS) announced on Wednesday, February 21, the launch of the DHS Traveler Redress Inquiry Program (DHS TRIP). Travelers can now

seek redress and resolve possible watch list misidentification issues with any of the department's component agencies at an easy to use and easy to access online location. DHS TRIP provides a way for legitimate travelers to address situations where individuals believe they have been incorrectly delayed, denied boarding, identified for additional screening, or have otherwise experienced difficulties when seeking entry into the country. The program also facilitates redress information sharing among the department's component agencies and creates internal performance measures to monitor progress. DHS TRIP enables travelers to outline their concerns in a single request via a secure Website. In addition to offering DHS TRIP, the department has taken a number of other steps to make the screening process more efficient and secure, to include the recent completion of a name-by-name review of the No-Fly list to ensure that only individuals currently posing a threat are included.

Traveler Redress Inquiry Program: <http://www.dhs.gov/trip>

Source: http://www.dhs.gov/xnews/releases/pr_1172073065966.shtm

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

Postal and Shipping Sector

Nothing to report.

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

Agriculture Sector

15. *February 21, Virginia Department of Agriculture and Consumer Services* — Equine herpes virus reported in Virginia. Under the direction of State Veterinarian Richard Wilkes, veterinarians with the Virginia Department of Agriculture and Consumer Services (VDACS) are currently quarantining six farms with horses that could have come in contact with a horse infected with a neurological form of Equine Herpes Virus-1 (EHV1). The Maryland Department of Agriculture is working with similarly-exposed animals in that state. The infected horse was treated at the Marion duPont Scott Equine Medical Center in Leesburg, VA, which is also under quarantine. Quarantines will restrict movement on and off the affected facilities. In addition, veterinarians are urging horse owners to observe strict hygiene control procedures. The disease first appeared in the U.S. in 2001, and Virginia had its first case in 2002.

EHV1 information: http://www.aphis.usda.gov/vs/nahss/equine/ehv/ehv_2005.htm

Source: <http://www.vdacs.virginia.gov/news/releases-b/022107equine.s.html>

16. *February 21, Dow Jones* — Canada cattle imports are documented and under control. Some imported Canadian cattle may have violated Washington state's regulations after entering the U.S., but the federal government believes it is accurately documenting trade, U.S. Department of Agriculture (USDA) officials said Tuesday, February 20. "These are not undocumented cattle," USDA Undersecretary Bruce Knight told Dow Jones Newswires. Knight is in charge of investigating whether there were any federal trade infractions, but stressed that it appears so far that only some state-level documentation was botched. The U.S. allows imports only of Canadian cattle younger than 30 months. Animals older than that are banned. So far in the USDA investigation, spokesperson Andrea McNally said, the bulk of problems found were

failures of feedlots to provide the Washington State Veterinarian's Office with copies of "movement permits" when cattle were sent to slaughterhouses. These notices, she said, are filed when cattle move from a feedlot to a slaughterhouse.

Source: <http://www.cattlenetwork.com/content.asp?contentid=107616>

17. *February 21, Associated Press* — **Hormone heist has authorities worried.** Surveillance video captured three thieves slipping onto E.J. deJong's California dairy farm under the cover of night. One used a bar to pry open the door to the farmer's office, where deJong stored thousands of drug-filled syringes used to boost milk production in his herd. They made quick work carting out their haul. In just one night, deJong lost about \$30,000 worth of the genetically engineered hormone rBST, or recombinant bovine somatotropin, in what police say was one of the most brazen, high-value heists to date. The three suspects still haven't been caught. Rural crime officials say vials of rBST are a favorite among thieves who resell the growth hormone for top dollar on the black market. Fewer dairy farmers use it these days and thefts have declined in recent years, but the sophistication and overall worth of the December break-in have alarmed authorities over the possibility of a larger hormone-peddling syndicate. "These kinds of crooks don't steal this stuff unless there's a market for it," said William Yoshimoto, a Tulare County prosecutor and project director for the Agricultural Crime Technology Information and Operations Network. "We're worried something is starting up again."
- Source: <http://www.cnn.com/2007/US/02/21/california.farm.ap/index.html>

18. *February 20, WJZ-TV (MD)* — **Thousands of Maryland fish destroyed because of disease.** Trout are raised in state hatcheries to be released into Maryland streams for fishermen to catch. But 80,000 trout are headed to the landfill to stop an outbreak of whirling disease at two Garrett County hatcheries. The parasite that causes the disease can deform fish and leave them spinning in the water. How the disease got into the hatcheries is unknown, although animals or people could have introduced it. The parasite enters very young trout triggering deformities and whirling. When the fish dies, spores from the parasite enter a small aquatic worm, where the cycle begins again.
- Source: http://wjz.com/pets/local_story_051163008.html

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

Food Sector

19. *February 21, Canadian Press* — **Salami products recalled.** Canada's food inspection agency says some salami products may have been tainted with salmonella. Siena Foods Ltd.'s Genoa and Calabrese salami may have been affected. The products have been distributed throughout Canada. There have been no reported illnesses associated with eating the affected meat. Salmonella can cause serious and sometimes deadly infections in young children, the elderly and people with weakened immune systems.
- Source: http://bodyandhealth.canada.com/channel_health_news_details.asp?news_id=11763&news_channel_id=1020&channel_id=1020&rot=11

20. *February 21, Xinhua (China)* — **U.S. baby food removed from market in Singapore.** Singapore's Agri-Food and Veterinary Authority (AVA) on Wednesday, February 21, ordered

a recall on one baby food product by U.S. Earth's Best following an alert from the U.S. Food and Drug Administration (FDA) that the baby food may be contaminated with Clostridium botulinum, which can cause botulism, a life-threatening illness. According to a joint statement by the Agri-Food and Veterinary Authority (AVA) and the Ministry of National Development, the product recall in the city-state is a precautionary measure as there have been no illnesses reported to date.

Source: http://news.xinhuanet.com/english/2007-02/21/content_5761544.htm

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

Water Sector

Nothing to report.

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

Public Health Sector

21. *February 21, Reuters* — Russia finds bird flu in new region, suspects more. Russia confirmed another outbreak of the H5N1 strain of bird flu on a farm in a southern region on Wednesday, February 21, and suspects two more outbreaks on farms near Moscow. Alexei Alexeyenko, spokesperson for animal and plant health watchdog Rosselkhoznadzor, said the H5N1 strain was identified in the republic of Adygeya, a region in the North Caucasus. Bird deaths also have been registered at farms in Dmitrov district, part of Moscow region, and Borovsk district in the Kaluga region, which borders the Moscow region to the south. Alexeyenko said he expected confirmation of the presence of the virus in these regions within the next two days. Outbreaks of H5N1 have so far been confirmed in Moscow's Sadovod pet market and in five districts of the Moscow region — Domodedovo, Odintsovo, Podolsk, Naro-Fominsk and Taldom.

Source: <http://www.alertnet.org/thenews/newsdesk/L21696295.htm>

22. *February 21, HealthDay News* — U.S. health-care costs to top four trillion dollars by 2016. Federal forecasters predict that U.S. health-care spending will double by 2016, to \$4.1 trillion per year. That's one-fifth of the nation's gross domestic product (GDP). Health spending in 2006 was projected at \$2.1 trillion, or 16 percent of the GDP. "There is a relatively modest and stable projection for 2006 to 2016, with an average growth rate of 6.9 percent," John Poisal, deputy director of the National Health Statistics Group at the Centers for Medicare and Medicaid Services (CMS), said during a teleconference. He noted that with projected growth rates falling slightly in 2006 and 2007, "that would result in five consecutive years of slowing growth." By 2016, Medicare spending is expected to more than double, reaching \$862.7 billion. U.S. prescription drug spending should reach \$497.5 billion by 2016, more than double the expected level for 2006. Prescription drug spending will grow at an average annual rate of 8.6 percent until 2016. The cost of hospital care is expected to climb to more than \$1.2 trillion by 2016, vs. \$651.8 billion expected for 2006.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/02/21/AR2007022100524.html>

23. *February 20, United Press International* — **United Kingdom conducts flu pandemic exercise.** The United Kingdom's government said Tuesday, February 20, it conducted an exercise to assess its capability to respond to an influenza pandemic. The exercise, known as Winter Willow, was conducted Monday, February 19, and Tuesday, February 20. It tested the ability of national, regional and local governments to manage the effects of an influenza pandemic that has resulted in widespread cases across the country. The Department of Health will use the findings in its overall pandemic flu preparedness plan.
Source: <http://www.upi.com/HealthBusiness/view.php?StoryID=20070220-094408-1474r>

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

Government Sector

24. *February 21, Batesville Guard Online (AR)* — **Board watches school buses.** Danny James watches 22 green triangles ratchet across his computer screen every school morning and afternoon. James told the Batesville School Board at its regular meeting Monday night, February 19, that each triangle is a real-time representation of a district school bus. Using the newly installed Edutracker global positioning system, the district's transportation coordinator can monitor every busload's location and speed as well as its number of stops and miles traveled. James and his crew can also spot buses that are driven recklessly and help drivers and students in case of an emergency. It is unusual to find a system like this at a district the size of Batesville, Superintendent Ted Hall said, but the system could be well worth its \$40,000 initial price tag if it prevents a disaster.
Source: http://www.guardonline.com/?module=displaystory&story_id=38454&format=html

25. *February 20, Federal Computer Week* — **President Bush swears in McConnell as new DNI.** At Bolling Air Force Base in Washington, DC, on Tuesday, February 20, President Bush made official the beginning of Michael McConnell's tenure as director of national intelligence (DNI). McConnell is now the second DNI since the post was created, replacing incoming Deputy Secretary of State John Negroponte. McConnell, a retired vice admiral in the Navy, was director of the National Security Agency from 1992 to 1996. Since then, he has been a senior vice president at Booz Allen Hamilton, leading projects related to computer network attack and defense responsibilities for the Defense Department. Previously, McConnell was intelligence director for the Joint Chiefs of Staff during the first Gulf War and led projects supporting the President's Commission on Critical Infrastructure Protection, focusing on the vulnerabilities of the banking and financial sector. In his speech, Bush said he has asked McConnell to continue reforming the intelligence community, focusing on integration, information sharing and collaboration. Bush also directed him to fix acquisitions problems, to "restore agility and excellence, and ensure that our nation invests in the right intelligence technologies."
Source: <http://www.fcw.com/article97714-02-20-07-Web>

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

Emergency Services Sector

26.

February 21, Valencia County News–Bulletin (NM) — **Responders learn what to do in rail emergency.** The New Mexico Rail Runner Express pulled into the Belen station Saturday, February 17, but it wasn't to pick up commuters. It was to give local law enforcement and emergency responders a hands–on look of what they would be dealing with in the event of a train disaster. Agencies from all over Valencia County were invited to attend the workshop Saturday that allowed them to see how the New Mexico Rail Runner Express commuter train works and what vital information they need to know in case of an emergency. The Rail Runner was parked at the Belen station for approximately two hours, and Equipment Maintenance Manager Anthony Ruiz went over the commuter train inside and out. Those who attended learned about everything from shutting down the train's engine to how to open the train doors when there's no power to how much fuel it carries and what to expect when removing windows to evacuate passengers. Besides the 450 volts of electrical power, there's 2,000 gallons of diesel fuel and air pressure lines to worry about, said Protective Security Advisor Rudy Holm of Homeland Security.

Source: <http://www.news-bulletin.com/news/69045-02-21-07.html>

27. *February 21, Daily Journal (MS)* — Emergency responders in Mississippi give plans a dry run. Four wounded students extracted from the scene of a school shooting, and a fatal injury to the shooter were the climax of a practice exercise at East Corinth Elementary School on Tuesday, February 20. But law enforcement and emergency responders had an intense interest in ensuring their plans for response in the case of a real emergency would work well. "Our goal was to see how our department reacted and worked with the other agencies to make sure our plan would work," said Corinth Police Chief David Lancaster. The drill's scenario was a reported school shooting, with victims to be taken by ambulance to the hospital for medical treatment. "We have a Crisis Management Plan and have had staff training by the Corinth Police Department for procedures if there's an emergency," said Corinth schools superintendent Lee Childress. "This is an opportunity to test the procedures and see if there are actions on the school's part or emergency responders' part that require adjusting to assure the safety of children in each of our schools." After taking numerous photographs from many angles and videotaping for several perspectives, participating agencies will gather to review what worked well and what may require improvements.

Source: <http://www.djournal.com/pages/story.asp?ID=237437&pub=1&div=News>

[[Return to top](#)]

Information Technology and Telecommunications Sector

28. *February 21, US–CERT* — Multiple vulnerabilities in Trend Micro ServerProtect.

US–CERT is aware of multiple stack–based buffer overflow vulnerabilities in the Trend Micro ServerProtect "stcommon.dll" and "eng50.dll" modules. Exploitation of these vulnerabilities may allow execution of arbitrary code with SYSTEM privileges.

US–CERT recommends users apply the ServerProtect 5.58 for Windows Security Patch 1–Build 1171 patch as soon as possible:

<http://www.trendmicro.com/download/product.asp?productid=17>

Trend Micro Vulnerability Response:

<http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034290>

NVD Vulnerability Summary CVE–2007–1070:

<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-1070>

Source: http://www.us-cert.gov/current/current_activity.html#tmbofs

29. *February 21, CRN* — **Google Desktop vulnerability fixed.** Google has fixed a serious vulnerability in its popular Google Desktop software that could allow remote attackers to access confidential data and gain full control over affected PCs. Google Desktop, which extends Google's Web search and indexing functions to local PC hard drives, is susceptible to a cross-site scripting attack (XSS) because of its failure to properly encode output data, according to researchers at security vendor Watchfire, which discovered the flaw in January. Google issued a fix for the vulnerability soon after being notified by Watchfire, and users are being automatically updated with the patch, according to a Google spokesperson. Although Google has fixed this XSS vulnerability, the fact that the online and offline connection with Google Desktop still exists means that the software could still be vulnerable, according to said Mike Weider, CTO of Watchfire.

Original report: <http://www.watchfire.com/news/releases/02-21-07.aspx>

Source: <http://www.crn.com/sections/breakingnews/dailyarchives.jhtml?articleId=197007769>

30. *February 21, SC Magazine* — **Microsoft takes down malicious MSN Messenger banner advertisements.** Banner advertisements that install malware onto the user's computer were left unnoticed for several days on the MSN Messenger service, according to researchers. The advertisements appear to promote a security application, known as Winfixer or ErrorSafe—said to identify and repair threats and other computer problems. The malware is downloaded and installed onto the user's machine without their authorization and announces fake security warnings to entice the recipient into buying a licensed copy of the product, according to security analysts. Microsoft has now acknowledged the problem and removed the advertisements, which were displayed in the contacts panel in its instant messaging program.

Source: <http://scmagazine.com/us/news/article/634699/microsoft-takes-down-malicious-msn-messenger-banner-advertisements/>

31. *February 20, Government Computer News* — **Many unknowns remain in move to IPv6.** On Tuesday, February 20, a panel of government and industry experts met during the IPv6 Tech Forum in Virginia to discuss uses for the new IPv6-enabled networks and the challenges users will face. The Department of Defense, along with civilian agencies, has set a goal of transitioning its networks to the next generation of Internet Protocols by July 2008. But a successful transition to IPv6 will merely establish parity with existing networks. The return on the investment will depend on how applications take advantage of the new functionality. Unfortunately, there still are many unanswered questions about what will happen when networks begin using IPv6. The federal government is a major driver in the industry's move to IPv6, because it has been requiring functionality for the new protocols in its networking equipment. The business rationale for moving to IPv6 will be improved productivity or functionality. The opportunity to strip proprietary protocols out of legacy systems and build everything on IPv6 should save money on licensing and simplified application development. But the steep learning curve in managing networks with the new protocols could delay these benefits.

IPv6 Tech Forum: <http://www.afcea.org/committees/technology/techforum/>

Source: http://www.gcn.com/online/vol1_no1/43184-1.html

Internet Alert Dashboard

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

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

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

Commercial Facilities/Real Estate, Monument & Icons Sector

32. *February 21, USA TODAY* — Louisiana levee plan leaves some helpless. State and federal plans for a massive hurricane protection bulwark for Louisiana would sacrifice dozens of coastal communities, some with thousands of residents, to the next Katrina-sized hurricane. The reason: Protecting them would cost too much. "We believe that it's probably not possible to provide adequate protection..." says Randy Hanchey of the state's Department of Natural Resources, which drafted one of the plans. The U.S. Army Corps of Engineers, ordered by Congress last year to design its own set of storm defenses, reached a similar conclusion, project manager Tim Axtman says. "The reality is, the cost of protection doesn't equate to what's there," he says. Most of the places that would be outside the new barriers are rural towns slung along the few remaining patches of high ground near the receding coast. A draft of the state's plan released this month shows new levees would exclude areas that were home to more than 20,000 people before hurricanes Katrina and Rita hit. The state and federal plans are due to be turned over to lawmakers this year.

Source: http://www.usatoday.com/news/nation/2007-02-20-la-levee-plan_x.htm

33. *February 21, Nevada Appeal* — Dynamite detonated behind old Wal-Mart building. Residents throughout downtown Fallon, NV, heard a loud explosion Sunday night, February 18, when the Explosive Ordnance Disposal team from NAS Fallon blew up a stick of dynamite fitted with a blasting cap and timed fuse, which was found by a man behind the old Wal-Mart building. Fallon Police Chief Russ Brooks said a man walking on the easement road south of the railroad tracks that leads to Western Nevada Community College notified police after finding the explosive. "He saw a white bag, and when he picked it up a stick of dynamite fell out. It had black tape around it and a blasting cap," said Brooks. Several concerns prompted studies throughout the afternoon and into the evening. Brooks said Southwest Gas has a pipeline in the area, and a jet fuel pipeline operated by Kinder Morgan runs nearby. Brooks said City Engineer Larry White arrived with maps of underground utilities to help decide where and how the device could be detonated. After the area was deemed safe, officers searched the road where the dynamite was found for evidence. They returned the next day to search in daylight.

Source: http://www.nevadaappeal.com/article/LF/20070221/News/1022100_33/-1/REGION

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

General Sector

34. *February 21, Associated Press* — States to crack down on metal theft. Stealing metal and selling it to scrap dealers has long been a way to make money, but with metal prices running

higher than usual, the problem has gotten especially bad, and now lawmakers in Illinois and at least a dozen other states are trying to stop some of the plundering of vacant houses, businesses, construction sites, churches, and even graveyards. They are pushing measures that would require scrap dealers to keep detailed records on those who sell them metal. The hope is that the paper trail will lead to arrests. For scrap-metal thieves, anything is fair game -- siding, gutters, spools of electric cable, pipes, even beer kegs. Some of the more brazen ones raid salvage yards, then sell the stolen metal back to the businesses. Among the proposals for cracking down on thefts: In Illinois, a measure would require scrap dealers to copy the driver's license or state ID of metal sellers and photograph the license plate and side of the seller's vehicle, along with the items purchased.

Source: <http://www.breitbart.com/news/2007/02/21/D8NE9GU81.html>

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

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.