Daily Highlights

- The Associated Press reports Xcel Energy has announced a consortium to study and plan ways to increase capacity and strengthen the high-voltage backbone regional transmission system connecting Wyoming, Colorado, New Mexico, and Arizona. (See item 3)

- Orlando International Airport officials, already scrambling to plug security gaps, had a new concern: sensitive documents detailing the airport's layout, fuel-storage facilities, communications systems, and power lines were found in a dumpster just east of the airport perimeter. (See item 16)

---

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

1. March 18, New York Times — Oil-rich nations turning attention to alternative fuels. Abu Dhabi, the capital of the United Arab Emirates (UAE), the fourth-largest OPEC producer with about 10 percent of the known oil reserves, is seeking to become a center for the development and implementation of clean-energy technology. Last year, the emirate launched the Masdar Initiative, which has signed up major oil and technology companies, universities around the world, and UAE ministries to help develop and commercialize renewable-energy technologies backed by hundreds of millions of dollars of Abu Dhabi's money. The UAE is only the most
serious among Persian Gulf oil-producing countries whose thirst for electrical power has
spawned efforts to find other sources of energy to save high-value fossil fuels for export. Most
Persian Gulf states get their water from desalinating gulf waters, an energy-intensive process.
With their populations growing rapidly, domestic consumption of oil is commanding a greater
share of production.

2. March 18, Associated Press — Mexico says oil monopoly struggling. Mexico's state oil
monopoly is in "critical" condition and needs to boost exploration and seek outside expertise to
replenish oil reserves that are currently set to last less than a decade, energy officials said
Sunday, March 18. President Felipe Calderon, however, said that there are no plans to privatize
the industry. Pemex's (Petroleos Mexicanos) proven reserves have fallen to the equivalent of
9.3 years of production from 9.7 years in 2005, and daily output declined last year by 2.3
percent to about 3.2 million barrels, officials said. "The situation of Petroleos Mexicanos is
critical and merits immediate attention," Pemex Chief Executive Jesus Reyes Heroles said.
Energy Secretary Georgina Kessel said Mexico must seek "complementary investment,"
especially in technology and scientific knowledge, in order to develop energy infrastructure
projects. Calderon said one option was to form strategic alliances to explore for new reserves in
deep waters off the Gulf of Mexico. Reyes Heroles said Pemex remains the most indebted oil
company in the world. He also said the company continues to be a target for fuel thieves, with
207 illicit openings discovered in pipelines or valves last year.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2007/03/
18/AR2007031800909.html

3. March 15, Associated Press — Xcel announces consortium to study Western transmission
lines. Major western utilities and a federal agency on Thursday, March 15, announced they will
study and plan ways to increase capacity and strengthen the high-voltage "backbone" regional
transmission system between Wyoming, Colorado, New Mexico and Arizona. "Historically, the
development of electric transmission has followed the announcement of new generating
sources," said Doug Jaeger, Xcel Energy vice president for transmission said. "This study is
unique in that we will develop a proactive plan to create the robust infrastructure needed to
support renewable expansion and other generation necessary for Colorado and the surrounding
region." Part of the study will include looking at whether five recently announced transmission
projects can become part of coordinate plans for the region.
Source: http://seattlepi.nwsource.com/local/6600AP_WST_Electricity_T
ransmission.html?source=rss

company Hokuriku Electric Power Co. admitted on Thursday, March 15, that it had covered up
a 1999 incident in which mishandling of nuclear fuel rods led to an unintended self-sustaining
nuclear fission chain reaction for 15 minutes. The news of the 15-minute "criticality" — an
unintended self-sustaining nuclear fission chain reaction — is likely to further dent public
confidence in Japan's nuclear power industry, already undermined by safety scandals over the
past decade. An official with Hokuriku's nuclear team admitted the company had not reported
the incident, which took place during a test while the unit was offline for a planned inspection.
Toshihiko Takahashi said that the incident may have breached laws governing nuclear plant
regulation. Hokuriku Electric said the mishandling of nuclear fuel rods caused the company's
Shiga No. 1 nuclear unit in central Japan to go into a "critical state" for 15 minutes in June 1999. "In a worst-case scenario, there might have been some radiation leakage to the outside," said Chihiro Kamisawa of the Citizen's Nuclear Information Center. "We were not looking at a Three Mile Island, but this accident highlights some serious technical problems," he added. Source: http://today.reuters.com/news/articlenews.aspx?type=worldNews&storyID=2007−03−15T105259Z_01_T75294_RTRUKOC_0_US−JAPAN−NUCLEAR.xml

Chemical Industry and Hazardous Materials Sector

5. March 19, North Jersey (NJ) — Methane leak keeps movie theater closed. The AMC Loews Ridgefield Park Theater in New Jersey remained closed Sunday, March 18, after a methane gas leak set off the theater's alarms Saturday. Police, fire and Hazmat officials responded to the leak shortly after 5:30 p.m. EDT Saturday. Moviegoers were soon evacuated from the theater. Fire officials ordered the theater closed while an investigation is pending. The source of the leak was not determined. Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFIZUVFeX0NyZmZ2JbDdmN3ZxZWVFRX15NzA5NjM2MyZ5cmlyeTdmNzE3Zjd2cWVIRUV5eTM=

6. March 18, New York Times — Suicide bombers using chlorine gas kill two and sicken hundreds in Western Iraq. Three suicide bombers driving trucks loaded with explosives and tanks of chlorine gas detonated their payloads in Anbar Province on Friday, March 16, killing at least two Iraqi police officers and wounding or sickening more than 350 people, the American military command said Saturday. Police and hospital officials, however, said that as many as eight people had been killed. Insurgents began combining explosives with chlorine gas and other chemicals in January in an effort to sow more fear and havoc among civilians, military officials say. Source: http://www.nytimes.com/2007/03/18/world/middleeast/18iraq.html?_r=2&ref=middleeast&oref=slogin&oref=slogin

Defense Industrial Base Sector

7. March 19, Federal Computer Week — New contracting policies respond to longstanding contracting concerns. Contractor performance awards and the role of lead systems integrators are near the top of the list of troublesome contracting issues that the Department of Defense (DoD) says it must get fixed. But the challenges DoD faces in reforming its billion-dollar contracting activities are familiar ones: the lack of clear financial metrics, the difficulty of maintaining a focus on reform, and the sheer size of the problem. “This is just gigantic,” said Kenneth Krieg, undersecretary of defense for acquisitions, technology and logistics. Krieg spoke to reporters last week about DoD’s latest plans to reform defense contracting. DoD plans to require officials at a more senior level to determine contract award fees. It wants to avoid paying for work that is deemed unsatisfactory. Officials will soon issue instructions for
implementing the new policy, Krieg said. Under new policies, awards and incentives will be linked to specific outcomes, such as cost, schedule and performance. DoD is also considering the idea of creating a fixed-award fee pool for which various contractors could compete.

Source: [http://www.fcw.com/article97963-03-19-07-Print](http://www.fcw.com/article97963-03-19-07-Print)

8. **March 15, GovExec — House passes contracting reform bill.** The House on Thursday, March 15, overwhelmingly approved legislation that would limit the use of certain types of federal contracts, boost oversight of procurement operations and take small steps to bolster the federal acquisition workforce. House members cleared the measure by a vote of 347–73, working from a version of the bill (H.R. 1362) nearly identical to that approved during a Tuesday markup by the Armed Services Committee. The legislation would require agencies to restrict their use of noncompetitive, sole-source and cost-reimbursement type contracts. Agencies could generally rely on a noncompetitive contract for only about eight months before replacing it with a competitively awarded agreement. They also would have to develop plans, with measurable goals, to minimize their use of noncompetitive and reimbursement contracts. Those plans would be reviewed by the Government Accountability Office, which would report on them to Congress. The bill also would require agencies to disclose their justifications for and approvals of noncompetitive contracts.


9. **March 19, InformationWeek — Chinese hackers stealing gamers' identities.** According to Symantec's latest Internet Security Threat Report, China has moved up into second place, behind only the United States, when it comes to the countries with the most amount of malicious cyber activity. When it comes to gamers, though, China has really focused its malicious efforts. Half of the world's eight million online gamers come from China, according to Vincent Weafer, senior director of Symantec Security Response. With that much gaming activity going on, it's creating a market for people to buy the identities of successful gamers. "Hackers are going after the digital identity, the people with high scores," says Weafer. He explains that some hackers, like most around the world, are looking to target Chinese gamers to empty their bank accounts. Others, however, are going after the high scorers so they can steal their online identities and sell them to less-skilled players who want to appear successful.


10. **March 19, CNET News.com — UK tax credits site to stay closed after fraud.** A UK tax credit Website that was closed down by fraudsters in 2005 will not be back online before next summer at the earliest and may never be reopened, the British government has said. The HM Revenue and Customs portal was targeted by criminals who stole the identities and personal details of almost 13,000 staff at the Department for Work and Pensions and Network Rail and exploited poor security and ID checks to make fraudulent online claims for tax credits. Dawn Primarolo, the government's paymaster general who is responsible for the tax service, told members at a Parliamentary Treasury select committee hearing last week that the Website may be too high risk to ever be reopened. "My judgment is that without proper identification checks
on the e−portal it should not be reopened," she said.

11. **March 19, Government Computer News** — **Hackers become more professional.** An analysis of Internet−based threats by Symantec Corp. shows that hacking continued its two−year trend toward criminalization in the last half of 2006, with data theft fueling a thriving underground economy. The United States has the highest number of command and control computers driving these bot networks, with 40 percent late last year, and the U.S. government is a primary source of data breaches. Agencies accounted for 25 percent of reported exposures of personal data. The number of infected computers used in malicious botnets increased by 29 percent in the last half of 2006 to just more than six million, but the number of command and control servers dropped by 25 percent. Symantec speculates that this is because the networks are consolidating. These fewer but larger networks also are becoming more interoperable, using suites of malicious code that can cooperate with each other. An initial compromise can be followed up with a variety of malicious tools that allow the user to exploit a computer, making the networks more dangerous and more valuable.
Source: http://www.gcn.com/online/vol1_no1/43339−1.html

12. **March 11, Sunday Times (UK)** — **Al Qaeda plot to bring down UK Internet.** Scotland Yard has uncovered evidence that al Qaeda has been plotting to bring down the Internet in Britain, causing chaos to business and the London Stock Exchange. In a series of raids, detectives have recovered computer files revealing that terrorist suspects had targeted a high−security Internet hub in London. The facility, in Docklands, houses the channel through which almost all information on the Internet passes in or out of Britain. The suspects, who were arrested, had targeted the headquarters of Telehouse Europe, which contains dozens of servers. Security experts say the plot against Britain’s Internet hub reflects the constantly changing threat from al Qaeda and related Islamic extremist groups. The Telehouse hub is nicknamed CTU after the counter−terrorist headquarters in the television series 24. It is designed to provide back−up power for all Britain’s vital network services in the event of a large−scale terrorist attack elsewhere. Eliza Manningham−Buller, head of MI5, set up the Centre for the Protection of National Infrastructure last month. It is a special MI5 unit to help to protect infrastructure sites from terrorist attacks, such as telecommunications, the Internet and key utilities such as oil, gas installations and nuclear power stations.
Centre for the Protection of National Infrastructure Website: http://www.cpni.gov.uk/
Source: http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece

[Return to top]

**Transportation and Border Security Sector**

13. **March 19, Associated Press** — **Jet loses engine part, lands safely in Florida.** A plane returned safely to Palm Beach International Airport shortly after takeoff after losing a piece of its engine cover, officials said. After JetBlue Flight 830 took off about 6 a.m. EDT on Sunday, March 18, the pilot radioed the airport that he had felt the plane vibrate and that he was returning, airport spokesperson Lisa De La Rionda said. The Airbus A320 was headed for New York's Kennedy International Airport and was carrying 150 passengers and six crewmembers.
14. March 19, Associated Press — US Airways tries to move weary, stranded travelers. Airport lines were still long Monday, March 19, but getting back to normal as US Airways tried to recover from a paralyzing ice storm that stranded thousands of travelers in Northeast cities over the weekend. About 100 people spent Sunday night at Philadelphia International Airport, down from about 1,000 after the storm hit on Friday, said airport spokesperson Phyllis VanIstendal. In Pittsburgh, the long lines were due to Monday's normally heavy business travel demand and "residual weather-related issues," an airport spokesperson said. US Airways, the dominant carrier at both hard-hit airports, reported Sunday that it was trying to find seats for 100,000 passengers system-wide whose travel had been interrupted by the storm that hit the Northeast. Many US Airways customers were diverted to its largest hub, Charlotte, NC, on Friday when the storm dumped snow, sleet, ice and freezing rain on Philadelphia, New York, and other Northeast cities, the airline said. Computer problems, airline staffing rules and other problems slowed US Airways' attempts to clear the backlog. Meanwhile, 275,000 passengers were already booked on US Airways flights on Sunday that were nearly sold out from the start in part because of spring break.


15. March 19, Department of Transportation — Federal Railroad Administrator visits Albany to launch track inspection project for New York State. In the wake of several recent accidents, the federal government on Monday, March 19, is launching a rail inspection project to check nearly 1,300 miles of track across New York State for flaws that might lead to a train derailment among other new measures designed to improve rail safety in the wake of several recent accidents, Joseph H. Boardman, the Administrator of the Federal Railroad Administration announced during a visit to Albany. Boardman explained that during the next two days a federal track inspection vehicle called the T–16 will inspect the heavily used CSX tracks from Albany to Buffalo, including the lines to Niagara Falls and to Ripley at the Pennsylvania border. The itinerary will take the T–16 through Oneida, Rochester, and Cheektowaga where major derailments have occurred in recent days and months. The inspection will measure whether the two track rails are level and if the width between the rails is acceptable to avoid derailments. The Administrator added that last month he directed another federal track inspection vehicle, known as the T–18, be used on CSX tracks in New York. In addition, FRA is performing a safety review of railroad bridges in western New York.

Source: http://www.dot.gov/affairs/fra1107.htm

16. March 15, Orlando Sentinel (FL) — Sensitive plans, maps found in OIA dumpster. Orlando International Airport (OIA) officials already scrambling to plug security gaps had a new concern to explain Friday, March 15: how sensitive documents detailing the airport's layout, fuel–storage facilities, communications systems, and power lines wound up in a dumpster. The documents, part of an OIA 20–year growth master plan updated in August 2004, are labeled "sensitive security information" that should not be released without a "need to know." Instead, the documents somehow made their way into a trash bin next to a warehouse owned by the Greater Orlando Aviation Authority just east of the airport perimeter. A teenage aviation enthusiast who was exploring the area around the warehouse two weeks ago came upon the discarded documents and collected them as a souvenir. A parent delivered the material to the Sentinel last week in the wake of recent reports about OIA security problems. The airport's top
security official, Robert Raffel, stressed that the binders contained planning documents that were widely distributed to airport managers, staff and planners — and were not the airport's ultra-sensitive security plan. Still, he has ordered airport-security officials to conduct random checks of dumpsters and will send out warnings to workers about proper handling and disposal of sensitive documents.

1707mar17%2C0%2C625703.story?coll=orl-home-promo)

17. **March 14, Sydney Morning Herald (Australia) — Lasers causing pilots to fly blind.** Federal Labor has called for an investigation into threats posed by laser lights after reports of them being aimed at passenger aircraft pilots flying over Sydney, Australia. News Ltd on Wednesday, March 14, reported at least two mid-air alerts were issued by pilots landing on Sydney's Kingsford Smith Airport on Monday night after a laser beam hit their cockpits. Opposition transport spokesperson Martin Ferguson has written to the Office of Transport Security and the aviation safety watchdog calling for action. "The Office of Transport Security and the Civil Aviation Safety Authority must investigate the threat posed to aviation security and safety by laser lights," Ferguson said. "They are sold as toys, but in the wrong hands they can cause temporary blindness and permanent eye damage." The Australian and International Pilots' Association said laws already were available to prosecute people if caught.


---

**Postal and Shipping Sector**

Nothing to report.

---

**Agriculture Sector**

18. **March 17, Billings Gazette (MT) — Rare form of scrapie found in sheep.** The Wyoming Livestock Board says a sheep from a flock in the northeastern corner of the state has tested positive for a rare form of the disease scrapie, the first time the particular strain has been found in the U.S. The U.S. Animal Plant Health Inspection Service notified the state Friday, March 16, that the ewe tested positive for a form of scrapie consistent with the Nor98 strain, first diagnosed in Norway in 1998. The ewe was slaughtered in Michigan as part of the U.S. Department of Agriculture's regular scrapie slaughter surveillance program and traced back to the Wyoming flock.


19. **March 17, Daily Journal (CA) — Herpes outbreak kills two horses in California.** Horsing boarding facilities on the coast are instituting a voluntary quarantine of horses after the first confirmed cases of a deadly form of the equine herpes virus in San Mateo, CA, were recently identified. Three stables in the Moss Beach and Montara area are under voluntary quarantine to
help stop the spread of the neurotropic form on equine herpes virus. The San Mateo County Farm Bureau reported the outbreak Friday, March 16. Three cases were identified at a boarding facility in Montara, north of Half Moon Bay on March 12. A four–year–old horse became feverish March 6. She began showing slight signs of ataxia on the evening of March 11th, and was unable to stand the next morning. At that time, one other horse in the paddock was also ataxic. Two other horses at the boarding facility have also tested positive, with one other pending.

Equine herpes information: [http://www.vet.uga.edu/vpp/IVM/ENG/ERD/EHV−4and1.html](http://www.vet.uga.edu/vpp/IVM/ENG/ERD/EHV−4and1.html)


20. **March 16, Animal and Plant Health Inspection Service — USDA begins implementation of additional potato surveillance measures.** The U.S. Department of Agriculture’s (USDA) Animal and Plant Health Inspection Service, and the Canadian Food Inspection Agency (CFIA), have developed a joint certification protocol for the potato cyst nematode and golden nematode for all seed potatoes traded between the U.S. and Canada. The initial phase of the protocol will begin on March 21, 2007, as the first step in implementing this surveillance. The protocol responds to the 2006 detections of the potato cyst nematode in the state of Idaho and the golden nematode in the province of Quebec, Canada. The goal of this protocol is to maintain the safe movement of regulated articles between the U.S. and Canada while continuing to protect against the spread of these nematodes. The first phase of the protocol will include sampling and testing of soil associated with tubers in storage facilities for all remaining 2006 seed potatoes shipped between the U.S. and Canada. All shipments between the U.S. and Canada must include a phytosanitary certificate with an additional declaration confirming that the lot was tested and found free of these pests. The next phase of bi–national potato surveillance will begin during the 2007 production year and will include extensive field surveys for seed potatoes.


21. **March 18, USA TODAY — U.S. food imports outrun FDA resources.** Late in October 2006, a truckload of cantaloupes was stopped as it crossed the Mexican border into Nogales, AZ. U.S. Food and Drug Administration (FDA) inspectors took samples from some melons for routine food–safety tests, and importer Timco Worldwide distributed about 5,000 others to four states, Timco says. Two weeks later, the FDA told Timco that its tests detected salmonella. Timco recalled the other melons within 24 hours in case they were contaminated, too. But it was too late, company officials say. All had been sold. Since then, five other U.S. companies have recalled more than 700,000 cantaloupes grown in Mexico and Costa Rica because FDA or company tests found salmonella. Fewer than half were recovered before being sold, the companies say. The cantaloupe recalls reveal a vulnerability in the nation's food–safety defenses: Imports are escalating, but the FDA's ability to inspect them and police their safety isn't keeping up, say former FDA officials, government watchdogs and food–safety experts. The FDA inspects about one percent of the imported foods it regulates, down from eight percent in 1992 when imports were far less common.

Millions of children eat in school cafeterias that don't get the twice-yearly health inspections required by Congress to help prevent food poisoning. Schools are supposed to get two visits from health inspectors every year. But one in 10 schools didn't get inspected at all last year, according to U.S. Department of Agriculture (USDA) data obtained by The Associated Press. Nearly every public school participates in the program, which is run by the USDA. Half of the nation's 60 million students eat lunches prepared in school. According to the USDA, of 94,132 schools reporting in the 2005–06 school year: Ten percent, or 9,498 schools, were not inspected at all; Twenty-nine percent, or 27,184 schools, were inspected once; Sixty-one percent, or 57,450 schools, were inspected at least twice; and no data was reported by 7,309 schools.

23. March 16, Minnesota Department of Agriculture — Consumer advisory on potato salad. The Minnesota Department of Agriculture (MDA) has issued an advisory for consumers to avoid eating selected lot codes of Coborn's, Cash Wise and Midwest Pride potato salad — sold in 89 stores in Minnesota, North Dakota, South Dakota, Wisconsin, Iowa, Michigan and Nebraska — due to concerns that the product may be contaminated with Listeria monocytogenes bacteria. There are no reports of illnesses associated with consumption of the product. DBC Foods manufactured the product which was distributed to the stores and has issued a voluntary recall. According to MDA Dairy and Food Division Director Kevin Elfering, the contamination was first detected in a product sample collected during a routine store inspection. MDA investigators are now working to determine the source of the contamination. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially serious disease.

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

24. March 19, Associated Press — Indonesian woman dies of bird flu. An Indonesian woman died of bird flu on Monday, March 19, a health official said, raising the toll in the country worst hit by the virus to 66. The 21-year-old victim died after two weeks of hospitalization in the East Java town of Surabaya, said Nyoman Kandun of the Health Ministry, adding that she had a history of contact with infected chickens. Indonesia is to host a meeting this month of Asian health ministers and World Health Organization officials to discuss bird flu and efforts to develop vaccines.
25. *March 18, Agence France-Presse* — Bird flu spreads in northern Nigeria's main city. The H5N1 bird flu virus is spreading among poultry farms around northern Nigeria's largest city, a senior veterinary official said Sunday, March 18. "The avian influenza virus is still spreading among poultry farms and it has so far affected 33 farms in seven districts," Shehu Bawa, head of Kano State's Committee on Avian Flu, said. More than 80,000 birds have been culled in Kano, Bawa added. Nigeria, the continent's most populous nation with some 140 million people, early this year reported west Africa's first human bird flu death.


26. *March 17, Associated Press* — Toddler contracts rare infection. A two-year-old Indiana boy and his mother contracted a rare and life-threatening infection from his soldier father's smallpox vaccination. The boy and his mother were being treated in a specially ventilated room at the University of Chicago's Comer Children's Hospital. The boy developed a virulent rash over 80 percent of his body earlier this month after coming in contact with his father, who had recently been vaccinated for smallpox before he was to be deployed overseas by the Army. Physicians said the infection was a rare condition called eczema vaccinatum, which has not been reported since at least 1990, when the military ended a previous program of smallpox vaccination.

Source: [http://apnews.myway.com/article/20070317/D8NTSS3O0.html](http://apnews.myway.com/article/20070317/D8NTSS3O0.html)

27. *March 16, U.S. Food and Drug Administration* — FDA clears rapid test for meningitis. The U.S. Food and Drug Administration (FDA) Friday, March 16, cleared for marketing a test that uses molecular biology to quickly detect the presence of viral meningitis. The when used in combination with other laboratory tests, will help physicians distinguish between viral meningitis and the less-common, but more severe, version of meningitis caused by bacteria. Meningitis is an infection of the cerebrospinal fluid surrounding a person's spinal cord and brain, causing inflammation of the tissues in these areas. The illness is diagnosed by testing the fluid obtained from a patient during a spinal tap. Typically, diagnostic tests for meningitis can take up to a week to get results. But results from the new test are available in two and one-half hours.


28. *March 19, Federal Computer Week* — Survey: Federal government faster to adopt telework than private sector. Federal agencies are beating the private sector in adopting telework through legislation, continuity of operations planning, and employee enthusiasm. Government agencies have been encouraged to adopt teleworking more rapidly than private-sector companies through policy development and established standards, according to a survey of 2,197 public and private-sector employees by CDW-Government Inc. of Vernon Hills, IL. In 2000, Congress passed a law requiring agencies to let eligible employees telework. Five years later, the Defense Base Closure and Realignment Commission moved numerous Department of Defense offices, which motivated many of these agencies to encourage teleworking in order to retain workers unwilling to move or commute further to work, said Robert Green, director of
CDW–G’s civilian sales. Policies also have eliminated excuses for federal managers to restrict teleworking, as more than half of federal employees are eligible to telework. In contrast, fewer than 16 percent of private–sector employees are actually given the opportunity, the survey found. Agencies also are ahead of the private sector in continuity of operations planning. The survey found that 75 percent of federal employees could continue working via telework if their offices closed due to a man–made or natural disasters, while only 33 percent of private–sector employees voiced confidence in their companies’ abilities to function out of the office.

29. March 17, Associated Press — FBI issues school–bus driver memo. Suspected members of extremist groups have signed up as school bus drivers in the United States, counterterror officials said on Friday, March 16, in a cautionary bulletin to police. Asked about the alert notice, the FBI's Rich Kolko said, "There are no threats, no plots and no history leading us to believe there is any reason for concern," although U.S. law enforcement agencies were asked to watch out for kids’ safety. The bulletin, parts of which were read to the Associated Press, did not say how often foreign extremists have sought to acquire licenses to drive school buses, or where. It was sent as part of what officials said was a routine advisory to local law enforcement. It noted "recent suspicious activity" by foreigners who either drive school buses or are licensed to drive them, a counterterror official said. Foreigners under recent investigation include "some with ties to extremist groups" who have been able to "purchase buses and acquire licenses," the bulletin says. But Homeland Security and the FBI "have no information indicating these individuals are involved in a terrorist plot against the homeland," it says. It also says, "Most attempts by foreign nationals in the United States to acquire school bus licenses to drive them are legitimate."

Emergency Services Sector

30. March 19, Federal Emergency Management Agency — FEMA funds Hazard Mitigation Plan for Port of New Orleans. A recently approved grant from the Federal Emergency Management Agency (FEMA) will help the state of Louisiana and the Port of New Orleans Board of Commissioners develop a hazard mitigation plan that will ensure port facilities are better protected against future storms, hurricanes or other potential disasters. Funding from this $49,155 Hazard Mitigation grant is earmarked to develop a hazard mitigation plan compliant with the Disaster Mitigation Act of 2000 (DMA 2000). DMA, which was established by Congress, emphasizes the need for States and communities to prepare for possible disasters by developing hazard mitigation plans for existing and future buildings. With 22 miles of wharves and terminals, the Port of New Orleans is one of America’s leading general cargo ports. It boosts the local economy by providing more than 160,000 jobs and contributing $800 million in taxes annually to the state.

31. March 18, South Florida Sun–Sentinel — Federal funds help fight terrorism. The city of Sunrise, FL, has received $750,000 in federal funds from the Department of Homeland Security
Sunrise was among six cities in Broward County selected last month for the federal government's Urban Area Security Initiative. The others are Fort Lauderdale, Hollywood, Miramar, Pembroke Pines and Coral Springs. The program is designed to bolster the preparedness of first responders to terrorist threats and strikes at the local level. The money will be allocated for the following, among others: Vehicle tag readers, which will be used to check license plates for vehicles registered as "wanted" and "watch listed"; two surveillance platforms which will allow authorities to monitor parking lots and other spots; a mass casualty response unit to provide medical supplies in large emergencies; and hazardous materials software to help manage incidents. The city also recently received $50,000 for two all-terrain vehicles and surveillance and other equipment under a separate grant from the Department of Homeland Security.


---

**Information Technology and Telecommunications Sector**

32. March 19, New York Times — **Researchers track down a plague of fake Web pages.** Tens of thousands of junk Web pages, created only to lure search-engine users to advertisements, are proliferating. Now, researchers have uncovered a scheme in which a small group, creating false doorway pages, works with operators of Web-based computers who profit by redirecting traffic passed from search engines in one direction and then sending advertisements acquired from syndicators in the opposite direction. Surprisingly, the researchers noted that the vast bulk of the junk listings was created from just two Web hosting companies and that as many as 68 percent of the advertisements sampled were placed by just three advertising syndicators. The researchers found that for some keywords like “drugs” and “ring tone,” more than 30 percent of the results from major search engines were fake pages created by spammers. They discovered that the average spam density—a measure of the percentage of Web pages that contain only advertisements—was 11 percent for 1,000 keywords they used in their research. The researchers’ specific findings included evidence that some blog-hosting services have permitted an explosion of phony doorway pages. The paper was published by Yi-Min Wang and Ming Ma, cybersecurity investigators in the Microsoft's research division, in collaboration with Yuan Niu and Hao Chen, computer scientists at the University of California, Davis.

Source: http://www.nytimes.com/2007/03/19/technology/19spam.html?_r=2&ref=technology&oref=slogin&oref=slogin

---

**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

Nothing to report.

General Sector

Nothing to report.

DHS Daily Open Source Infrastructure Report Contact Information


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.